UNIVERSIDAD NACIONAL DE INGENIERIA

DIRECCION DE ESTUDIOS DE POSGRADO

MAESTRIA INFORMÁTICA EMPRESARIAL

Tesis para la obtención del grado de

Máster

Informática Empresarial

"Aplicación de Gestión de Riesgos Tecnológicos basada en la norma ISO/IEC 27005 en el área de Base de Datos y Sistema Operativo de la Dirección de Informática y Sistemas de la DGI."

Elaborado por:

- ✓ Ing. Judith Navarro Ordeñana

Tutor de tesis:

- ✓ Msc. Juan Bosco Ordoñez

Managua Nicaragua MARZO 2019

DEDICATORIA

Dedico este gran logro a mi Padre Celestial, por haberme guiado en todo este proceso, por darme la sabiduría y los recursos que necesité para culminar y seguir avanzando en mi vida profesional.

A mi amado esposo Msc. Gabriel Lacayo por su apoyo incondicional, por sus palabras de ánimo, por tomar de mi mano y levantarme en mis momentos más duros y aconsejarme en todo momento.

A mi mejor amiga Msc. Josseling Jasmina Alemán Guido por todos los momentos compartidos en el transcurso de nuestra maestría, por todas esas veces que trasnochamos para dar lo mejor en todos nuestros trabajos y que a pesar de tener diferentes opiniones, siempre nos lográbamos comprender.

AGRADECIMIENTO

Primeramente, agradezco al buen Gobierno de Nicaragua que me brindó la oportunidad de crecer y desarrollarme como profesional, a mis compañeros de labores muy cercanos de la Dirección General de Ingresos que gracias al compañerismo, amistad y apoyo moral han aportado en un alto porcentaje en mi crecimiento personal y profesional.

Agradezco también a mi asesor de tesis Msc. Juan Bosco Ordoñez por haberme brindado la oportunidad de recurrir a su capacidad y conocimiento científico, así como también el tiempo que dedicó en todo este proceso.

RESUMEN

Este documento presenta la aplicación de gestión de riesgos tecnológicos basada en la norma ISO/IEC 27005 en el área de Base de Datos y Sistema Operativo de la Dirección de Informática y Sistemas de la DGI con el fin de reducir el impacto de los riesgos a nivel físico, lógico y organizacional, mediante la estructura de una metodología hibrida Ciclo de Deming y Norma ISO/IEC 27005, identificando los activos más importantes del área en función de los objetivos de la organización, posteriormente son evaluados para aplicar el tratamiento del riesgo y finalmente se muestran los resultados obtenidos y las conclusiones de la gestión de riesgo con la metodología adaptada.

Tabla de contenido

Lista de Ilustraciones

Lista de Tablas

1. INTRODUCCIÓN

La Dirección General de Ingresos (DGI), es una institución descentralizada con autonomía administrativa y financiera, cuyo objeto es aplicar y hacer cumplir las leyes, actos y disposiciones que establecen o regulan ingresos a favor del estado, que están bajo la jurisdicción de la Administración Tributaria.

La visión de la DGI es ser una administración tributaria profesional, ágil y sencilla al servicio del pueblo nicaragüense. Por otro lado, su misión es recaudar los tributos internos con equidad, transparencia y eficiencia, promoviendo la cultura tributaria y cumpliendo con el marco legal, aportando al gobierno recursos para el desarrollo económico y social del país. Por tal razón la División de Informática y Sistemas de la DGI, siendo esta un eslabón de apoyo tiene como misión interna hacer cumplir los objetivos y metas de la organización alineados con las tecnologías de información, disponiendo de los recursos tecnológicos y servicios como la ventanilla electrónica tributaria, la cual debe mantenerse disponible las 24 horas, así como los diferentes sistemas que se derivan para el cumplimiento legal de los tributos.

La División de Informática y Sistemas (DIS) de la Dirección General de Ingresos se encuentra dividida en:

- Área de Sistemas Tributarios
- Área de Control de Calidad
- Área de Apoyo Tecnológico

Específicamente el área de Apoyo Tecnológico se divide en:

- Unidad de Base de Datos y Sistemas Operativos.
- Comunicaciones y Redes.
- Soporte Técnico.

El Área de Base de Datos y Sistema Operativo (UBDSO), es la encargada de la ejecución, mantenimiento y administración de las bases de datos de la institución, ejecución de sentencias, así como el mantenimiento y revisión de los servidores de hardware y software. Los recursos tecnológicos tangibles e intangibles que dispone la DGI, a diario son expuestos a diferentes cambios y por ende riesgos que pueden incidir sobre las metas y objetivos organizacionales y ser causa de otro tipo de riesgos al ser intrínseco al uso de tecnología. Por ello el daño, interrupción, alteración o falla derivada del uso de TI puede implicar pérdidas significativas en la organización, pérdidas financieras, multas o acciones legales, afectación de la imagen de una organización y causar inconvenientes a nivel operativo y estratégico.

A través de la Norma ISO/IEC 27005 de gestión de riesgos tecnológicos se identificaron, evaluaron y categorizaron los posibles riesgos que afectan directa o indirectamente en el Área de Base de Datos y Sistema Operativo de la Dirección de Informática y Sistemas de la DGI sobre la infraestructura (nivel físico), los sistemas de información (nivel lógico) y las medidas organizacionales (factor humano) desde la perspectiva de tecnologías de la información (TI), así como los posibles planes de mitigación para los mismos.

2. ANTECEDENTES

En sus inicios la DGI administraba los impuestos de forma cedular, existiendo una Dirección para cada tipo de impuesto (Dirección de Impuesto de Ventas y Servicios ISV, Dirección de Impuesto a la Renta IR, etc.). El contribuyente tenía un número de cuenta por cada impuesto, para efectuar sus transacciones tributarias. Con la Ley Creadora del Registro Único del Contribuyente publicada en la Gaceta, Diario Oficial No. 246 del 30 de octubre de 1981, se establece un número único para todas las transacciones tributarias, con lo que nace la Cuenta Única, y el contribuyente empieza a ser atendido por procesos: Declaración, Pago, Solvencia, etc., independientemente del impuesto.

Debido a las grandes filas que se atendían en las diferentes administraciones de rentas, la DGI amplio su visión y decidió actualizarse con nuevas tecnologías facilitando el servicio y la atención a los contribuyentes. En el 2006 nace la VET, facilitando a los contribuyentes el pago de sus impuestos desde cualquier lugar y en cualquier momento, abriendo las puertas al desarrollo tanto en tecnología como recursos humanos para seguir ampliando los diferentes entes reguladores que se derivan de la recaudación de tributos.

Esta nueva experiencia en la División de Informática y Sistemas (DIS), permitió fortalecer su estructura tecnológica, física y profesional. Desarrollando sitios más seguros y aplicando restricciones a nivel interno y externo de los puntos de accesos de navegación. Sin embargo, la magnitud de datos que se almacenan actualmente en las bases de datos principales de la DGI, se ensamblan en tecnología vieja y desactualizada, siendo esta vulnerable y con riesgos latentes que pueden impactar de forma negativa las TI.

En el Área de Base de Datos y Sistema Operativo, el término de gestión de riesgos no existe en documentos o informes, debido al descuido y atención de las distintas amenazas y vulnerabilidades que tiene la TI dentro del Área de Base de Datos y Sistema Operativo, en la mayoría de los casos los riesgos se materializan, debido a que no hay un control y seguimiento de estos. Actualmente la Gestión de riesgos tecnológicos, tanto

en el nivel lógico, físico y personal, se realiza de forma empírica. Por lo que se ve la necesidad de proponer la Norma ISO/IEC 27005 de gestión de riesgos tecnológicos en el Área de Base de Datos de la Dirección de Informática y Sistemas de la DGI que lleve un control y seguimiento de los mismos, identificando los riesgos más relevantes y que afectan los objetivos de la organización, evaluándolos y categorizándolos para darle un tratamiento dependiendo del nivel de madurez en que se encuentren.

A continuación, se mencionan algunos estudios realizados sobre Gestión de Riesgos basados en la Norma ISO/IEC 27005:

Caso 1: (García Porras, Huamani Pastor, & Lomparte Alvarado, 2018) La adaptación de la norma ISO/IEC 27005 fue implementado en el proceso de ventas de una PYME peruana del sector cerámicos, demostrando un fácil uso, y logrando identificar los controles necesarios para reducir el riesgo.

Caso 2: (Killkana Técnica, 2017) El autor presenta una metodología integral para la gestión de riesgos informáticos basándose en los estándares mundialmente aceptados como son ISO 31000 e ISO/IEC 27005, los mismos que indican los requerimientos para una gestión adecuada de riesgos; este estudio ofrece una oportunidad para hacer más avances en una importante y creciente temática como lo es la seguridad informática en determinados dominios, teniendo en consideración la identificación, evaluación y gestión de riesgos para una determinado tipo de organización, ya que se debe considerar que no todas las empresas u organizaciones tienen las mismas necesidades de seguridad, pues sus riesgos varían de acuerdo a su localización, su naturaleza, estructura y los procesos que se manejan así como los activos de información y controles que disponen; considerando además el enfoque e importancia que los directivos de una organización tienen respecto a la seguridad de su información y la situación o estado actual de una empresa en cuanto a seguridad informática se refiere.

3. PLANTEAMIENTO DE LA SITUACIÓN

El siguiente estudio, se aplicará en la Dirección General de Ingresos, específicamente en el Área de Base de Datos y Sistema Operativo de la Dirección de Informática y Sistemas de la DGI, tomando en cuenta como campo de acción los diferentes riesgos que se identifiquen sobre la infraestructura (nivel físico), los sistemas de información (nivel lógico) y las medidas organizacionales (factor humano) desde la perspectiva de tecnologías de la información (TI).

El Área de Base de Datos y Sistema Operativo cuenta con una infraestructura de equipos muy variada, ya que se encuentra en una etapa de renovación de equipos que han estado en funcionamiento por más de 10 años, adquiriéndose equipos con última tecnología para almacenamiento, virtualización, nuevos cortafuegos y equipos de conmutación de red; lo cual ha conllevado a superar algunas dificultades de compatibilidad, configuración y administración. Sin embargo, no está exenta a riesgos, vulnerabilidades y amenazas sobre la infraestructura (nivel físico), los sistemas de información (nivel lógico) y las medidas organizacionales (factor humano) desde la perspectiva de tecnologías de la información (TI).

En base a lo anterior se mencionarán algunos ejemplos de riesgos que se han materializado en el Área de Base de Datos y Sistema Operativo, provocando retrasos en la atención y calidad de los servicios.

La problemática que usualmente ocurre en el Área de Base de Datos y Sistema Operativo, es que los sistemas que están de cara al contribuyente no estén disponibles en fecha límite para el pago de impuestos, la cual produce suspensión en sus operaciones normales, trayendo como consecuencia retraso en los pagos de forma presencial y a través de la Ventanilla Electrónica Tributaria (VET).

Actualmente las versiones existentes de algunos de los gestores de bases de datos y servicios web, que se están ejecutando en los servidores de la DIS, están desactualizados, motivo por el cual no tienen soporte técnico por parte del proveedor,

siendo esto uno de los problemas que más preocupa en la base de datos principales.
Otro de los problemas es que la DGI ha adquirido equipos nuevos de hardware para máquinas virtuales que no son totalmente compatibles con la plataforma de administración de software de las mismas y en algunos casos se presentan inconsistencias por la versión del sistema operativo instalado.

También podemos encontrar inconsistencias en programas que se ejecutan en NATURAL[1] y en PHP[2] dado que algunos de estos programas que deberían de estar ejecutándose en un ambiente de producción lo hacen en ambientes de desarrollo provocando que estos estén ralentizando los servicios.

Por último, algunas consultas extensas de NATURAL que se ejecutan en programas principales de producción provocan colas y ralentizan los servicios, esto es más evidente en las fechas límite (entiéndase la fecha límite para la declaración y pago de impuestos) provocando que los sistemas que están de cara al contribuyente no estén disponibles para el pago de impuestos.

En base a lo mencionado anteriormente, la Norma ISO/IEC 27005 tiene muchas ventajas, ya que es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de su organización, así también permite valorar su entorno e identificar cuáles son los riesgos que pueden tener mayor impacto así como la probabilidad de ocurrencia, cómo detectarlos y categorizarlos para darle un control y seguimiento a través de la evaluación de posibles escenarios de forma cualitativa y cuantitativa adaptándolo a la TI del Área de Base de Datos y Sistema Operativo.

1 NATURAL es un lenguaje de cuarta generación creado por *Software AG*®.
[2] PHP, sigla recursiva en inglés de PHP: **Hypertext Preprocessor** (procesador de hipertexto), es un lenguaje de programación de propósito general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico.

4. OBJETIVOS

4.1 Objetivo General

Aplicar la Norma ISO/IEC 27005 de gestión de riesgos tecnológicos en el Área de Base de Datos y Sistema Operativo de la Dirección de Informática y Sistemas de la DGI para reducir el impacto de los riesgos a nivel físico, lógico y organizacional.

4.2 Objetivos Específicos

1. Realizar un diagnóstico del contexto de la organización articulando sus objetivos estratégicos con los parámetros externos e internos que inciden en la gestión de riesgos tecnológicos en el Área de Base de Datos y Sistema Operativo de la Dirección de Informática y Sistemas de la DGI.

2. Disminuir la ocurrencia de eventos asociados a vulnerabilidades, amenazas y riesgos identificados en el Área de Base de Datos y Sistema Operativo de la Dirección de Informática y Sistemas de la DGI mediante la aplicación de controles efectivos, basados en la Norma ISO/IEC 27005 de gestión de riesgos tecnológicos.

3. Contribuir en los procesos de toma de decisión a nivel gerencial mediante un plan de protección y tratamiento de riesgos tecnológicos en el Área de Base de Datos y Sistema Operativo de la Dirección de Informática y Sistemas de la DGI basado en la Norma ISO/IEC 27005.

5. JUSTIFICACIÓN

La información es el elemento más valioso para cualquier organización o persona, hoy en día es un instrumento para crear ventaja competitiva (Gabalán-Coello, 2015). Sin embargo, pese a la falta de conocimiento sobre cómo protegerla adecuadamente, o a la complejidad de las normas internacionales que indican los procedimientos para lograr un adecuado nivel de protección, muchas organizaciones omiten el grado de importancia que concibe la gestión de los riesgos tecnológicos, ya que al usar tecnología en su actividad diaria y como parte de sus procesos de negocios, se encuentran expuestas a este tipo de riesgos; por ello pueden afectar la actividad propia de las mismas y ser fuentes de pérdidas con daños considerables.

Aplicando los conceptos mencionados, dentro de la DIS el Área de Base de Datos y Sistema Operativo, está sensiblemente expuesta a afectaciones directas e indirectas, consecuencia de la falta de gestión de los riesgos tecnológicos, ya que no se identifican claramente cuáles son los activos principales de la empresa, para evaluarlos y dar seguimiento a los mismos. Todo se realiza de forma empírica.

En base a la problemática que actualmente vive la División de Informática y Sistemas de la DGI, se ve la necesidad de aplicar la Norma ISO/IEC 27005 de gestión de riesgos tecnológicos, apoyado con la norma ISO/IEC 31000 las cuales se adaptarán según las necesidades o problemáticas que se identifiquen durante el estudio. Los beneficios que aporta es que al identificar y evaluar posibles riesgos robustece su protección a nivel físico (lo correspondiente a infraestructura, incluyendo la tecnológica), nivel lógico (sistemas de información y software) y factor humano (toma de medidas organizacionales); además permite buscar estrategias que ayuden a la alta dirección en la toma de decisiones cuando un riesgo es materializado.

Esta norma a su vez permite la elaboración de planes de mitigación de riesgo, según su nivel de criticidad con el fin de cumplir con los objetivos de la organización y asegurar la información crítica; adicionalmente la gestión adecuada de los riesgos permite evitar en gran medida la ocurrencia de incidentes y con ello evitar la activación de planes de mitigación ante un riesgo materializado.

La Norma ISO/IEC 27005, se centra en los principios de confidencialidad, integridad y disponibilidad, cada uno equilibrado de acuerdo con los requisitos operativos. (Shanthamurthy, 2011) . La aplicación de la misma contribuye a disminuir el número de riesgos que están en un estado crítico pasando a un estado aceptable o bien manteniéndose en un estado estable.

6. MARCO TEÓRICO

En los últimos años la tendencia sobre la importancia de la información ha sido creciente, Sin embargo, las gestiones del día a día dentro de las organizaciones no permiten ver más allá, en cuanto a gestión de riesgos se refiere, ya sea por falta de recursos o por falta de conocimiento e interés sobre las consecuencias que pueden ocurrir en casos inesperados sobre todo en información expuesta a ataque maliciosos y devaluación de la organización, deteriorando la confianza, el valor, la integridad y disponibilidad de los servicios que ofrecen dichas organizaciones.

Un estudio de la Unidad de Inteligencia de **The Economist** (Franco, 2009) revela datos sobre el peligro que corre el futuro de las organizaciones si no se toman medidas correctivas en cuanto a la gestión de riesgo. En el reporte, llamado “Más allá de llenar casillas: una nueva era para el gobierno de riesgo”, se realizaron preguntas a 364 profesionales de riesgo, quienes se quejaron de la baja calidad de los datos, la tecnología inadecuada y la falta de pericia.

Y es que, en general, los hallazgos de la investigación demuestran que en las empresas hacen falta no solo recursos, sino también pericia en la alta gerencia, lo que, teniendo en cuenta que una gran porción de los encuestados dijo que la cultura de riesgo depende de una dirección fuerte desde arriba, significa que hay un panorama poco alentador para las compañías en cuanto a fortalecer una mayor conciencia y entendimiento del riesgo dentro de su negocio.

Lo anterior dicho, sintetiza el contenido del presente **Capítulo I,** definido como una investigación documental que recupera y trasciende reflexivamente el conocimiento acumulado descrito y contextualizado a través de distintos hallazgos de estudios, experiencias previas, referencias teóricas y perspectivas metodológicas relacionados al objeto de estudio: “Aplicación de Gestión de Riesgos Tecnológicos basada en la Norma ISO/IEC 27005 en el Área de Base de Datos y Sistema Operativo de la Dirección de Informática y Sistemas de la DGI.”

Basado en lo anterior, se realizó un cuadro comparativo de las normas relacionadas a Gestión de Riesgos Tecnológicos. Las siguientes normas contienen disposiciones que, al ser citadas en este texto, constituyen requisitos de esta norma ISO 27005.

Tabla 1 Tabla comparativa de Normas

ISO 27005 2014	ISO 27002 2005	ISO 27001 2013	ISO 3100 2009
proporciona directrices para la evaluación y el tratamiento de los riesgos de la seguridad de la información. Le da el know-how para identificar los activos, las amenazas y las vulnerabilidades, evaluar las consecuencias y la probabilidad, calcular el riesgo, etc. Y es totalmente compatible con la norma ISO 31000. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. (ISO 27000.ES, s.f.)	Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. (Kosutic, s.f.)	Enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI. Asi mismo se enfoca en la evaluación y tratamiento de los riesgos de una manera semántica, transparente y creíble dentro de cualquier ámbito y contexto. (ISO 9001:2015, 2016)	Principios y directrices genéricas para la Gestión de Riesgos (GR) de cualquier tipo en las organizaciones. ISO 31000 no proporciona metodologías o exclusivas, ya que el tratamiento del riesgo es general. Aborda cualquier tipo de riesgos y no profundiza en ninguno de ellos. (ISOTools, 2017)

Considerando el cuadro comparativo de la figura anterior se justifica que la selección de la Norma ISO/IEC 27005, es bastante completa y flexible para su desarrollo e implementación en área de base de datos, cabe destacar que esta noma es compatible y esta correlacionada a un conjunto de normas que la complementan.

6.1 Diseño metodológico

Para la metodología se utilizara un modelo hibrido: el modelo PHVA[3] alineado con la Norma ISO/IEC 27005, la que contendrá todo el contenido y desarrollo de la gestión de riesgos tecnológicos del área de Base de Datos.

A continuación, se describen ambos modelos:

PHVA

PLANIFICAR: Se establecen los objetivos, procesos y procedimientos para el proceso de gestión de riesgos tecnológicos. La finalidad de la planeación es la entrega de resultados acordes con las políticas y objetivos globales de la organización.

Así mismo, se establece el plan de comunicaciones y el análisis del contexto organizacional actual para definir el alcance de la gestión de riesgos tecnológicos.

HACER: Corresponde a la implementación y operación de los controles, procesos y procedimientos (incluye la operación e implementación de las políticas definidas), lo correspondiente a la valoración y tratamiento de los riesgos.

VERIFICAR: Evaluar y medir el desempeño de los procesos contra la política y los objetivos de seguridad e informar sobre los resultados.

ACTUAR: Establecer la política para la gestión de riesgos tecnológicos e implementar los cambios requeridos para la mejora de los procesos. Como parte de las fases verificar y actuar, se incluye el monitoreo y mejora continua, donde se verifican los cambios y el cumplimiento de los indicadores que fueran establecidos desde la planificación.

---

3 Ramírez, A., Ortiz, Z. (2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. En: *Ingeniería, Vol. 16, No. 2, pág. 56-66*

Metodología según norma ISO 27005[4]

El proceso de la gestión de riesgos se describe en las siguientes 6 cláusulas de la Norma ISO/IEC 27005: 2008

Tabla 2 proceso de la gestión de riesgos de la Norma ISO/IEC 27005 : 2008

1 Establecimiento del contexto	Objetivos Alcance
2 valoración de riesgos:	Identificación de riesgos: determinar qué puede provocar pérdidas en la organización Estimación de riesgos: utilizar métodos cuantitativos o cualitativos de los riesgos identificados, teniendo en cuenta los activos, las amenazas y las salvaguardas, Evaluación de riesgos, que consiste en comparar los riesgos estimados con los criterios de evaluación y aceptación de riesgos definidos en el establecimiento de contexto.
3 Tratamiento de riesgos	Define la estrategia para tratar cada uno de los riesgos valorados: reducción, aceptación, evitación o transferencia.
4 Aceptación de riesgos	Se determinan los riesgos que se decide

[4] Alessandro Deidda, ISO/IEC 27005:2008 – A New Standard for Security Risk Management, 16 Jul 2009, tomado de url: https://www.symantec.com/connect/blogs/isoiec-270052008-new-standard-security-risk-management

	aceptar y la justificación correspondiente a cada riesgo aceptado.
5 Comunicación de riesgos	Intercambio de información sobre los riesgos en los grupos de interés
6 Monitorización y revisión de riesgos	Actualización del análisis de riesgo

En línea con el estándar **ISO/IEC 27005:2008**, el proceso de gestión de riesgos se considera iterativo, siguiendo el ciclo de Deming

Tabla 3 Metodología hibrida (Ciclo Deming y Norma ISO/IEC 27005)

<table>
<tr><th>PHVA</th><th colspan="2">Norma ISO/IEC 27005</th></tr>
<tr><td rowspan="7">Planear</td><td colspan="2">Definir plan de gestión de riesgos</td></tr>
<tr><td colspan="2">Establecimiento del contexto</td></tr>
<tr><td>Identificación del riesgo</td><td rowspan="3">Valoración Riesgo</td></tr>
<tr><td>Estimación del riesgo</td></tr>
<tr><td>Evaluación del riesgo</td></tr>
<tr><td colspan="2">Desarrollar el plan de tratamiento del riesgo</td></tr>
<tr><td colspan="2">Aceptación del riesgo</td></tr>
<tr><td rowspan="2">Hacer</td><td colspan="2">Implementar el plan de tratamiento</td></tr>
<tr><td colspan="2">Implementar el plan de comunicación del riesgo</td></tr>
<tr><td>Verificar</td><td colspan="2">Monitoreo y revisión del riesgo</td></tr>
<tr><td>Actuar</td><td colspan="2">Mantener y mejorar el proceso de gestión</td></tr>
<tr><td colspan="3">Proceso de gestión de riesgos</td></tr>
</table>

posibilita la implementación, monitorización y mantenimiento de las actividades de la gestión de riesgos tecnológicos, optimizando los procesos y emprendiendo un camino hacia la excelencia e integración con otras normas como: la norma ISO 31000, la ISO 27001, e ISO 27001. Todo ello de una forma sencilla gracias a su estructura por módulos. (ISOTools, 2015)

El autor (Castro, 2011) es su estudio define que el establecimiento del contexto, la valoración del riesgo, el desarrollo del plan de tratamiento del riesgo y la aceptación del riesgo es parte de la fase de "planificar" del ciclo de Deming. En la fase de "hacer", se implementan las acciones y los controles que son necesarios para reducir el riesgo hasta un nivel aceptable, de acuerdo con el plan de tratamiento del riesgo. En la fase de "verificar", los directores determinarán la necesidad de revisiones de las valoraciones y del tratamiento del riesgo a la luz de los incidentes y los cambios en las circunstancias. En la fase de "actuar", se lleva a cabo todas las acciones que son necesarias, incluyendo la aplicación adicional del proceso de gestión del riesgo en la seguridad de la información.

Una de las referencias teóricas y perspectivas metodológicas basado en el estándar **AS/NZS 4360:2004** relacionados al objeto de estudio: “Aplicación de Gestión de Riesgos Tecnológicos basada en la Norma ISO/IEC 27005” mencionan los principales aspectos a considerar en el proceso de gestión de riesgo permitiendo identificar de una forma más practica la información que se requiere para la aplicación de la Norma ISO/IEC 27005:

- **Establecimiento del contexto:**
    - Definición de objetivos
    - Identificación de grupos de interés
    - Definición de criterios para el análisis de riesgos
    - Definición de elementos clave
- **Identificación de riesgos**
    - ¿Qué puede ocurrir?
    - ¿Cómo puede ocurrir?
- **Análisis de riesgos**
    - Revisar controles
    - Posibilidades
    - Consecuencias
    - Nivel del riesgo
- **Evaluación de los riesgos**

    - Evaluar los riesgos
    - Priorizar los riesgos
- **Tratamiento de los riesgos**
    - Identificar opciones (reducción, aceptación, traspaso, evitación)
    - Seleccionar las mejores estrategias
    - Desarrollar planes de tratamiento de riesgos
    - Implementar los planes

6.2 Diagnóstico del contexto de la organización

Varios estudios revelan que el establecimiento del contexto dentro de una organización, delimita el alcance de la gestión del riesgo. Según (Instituto Nacional de Ciber Seguridad, s.f.) “Es esencial que la gestión de riesgos se integre tanto con el resto de áreas de la empresa como con su entorno externo. Por tanto, hay que determinar los condicionantes tanto internos como externos que definen el marco de trabajo. A nivel interno se tendrán en cuenta: la cultura, recursos, procesos y objetivos del negocio. A nivel externo se consideran diferentes aspectos relativos al entorno social, económico o legislativo”.

Lo mencionado anteriormente se categoriza en activos primarios (críticos) y activos secundarios (apoyo).así como lo describe (Surridge, Bassem , Xiaoyu, Ajay , & Panos) Primario, se soportan activos como procesos de negocio e información. Por activos secundarios tales como hardware, software, redes, Personal, espacios físicos y estructura organizativa. En el estudio refiere que: “Los procesos críticos de la empresa son aquellos en los que se genera el valor principal para el cliente”.

Apropiando la teoría y otros estudios (Breier, 2014) fundamentan que esta información es útil para las siguientes fases de la gestión de riesgo, por lo que el administrador de seguridad puede centrarse solo en importantes procesos. Existen pocos papeles y herramientas de software implementando con el estándar ISO/IEC 27005:2011. Usualmente ellos proponen métodos de valoración simples, basados en una escala de medición discreta y enfoques cualitativos. Por ejemplo, proponen la valoración en

términos de "ninguna", "baja", "media" o "alta" importancia de un activo para la organización. También cabe mencionar que la identificación de las relaciones de dependencia entre activos y recursos de información es clave en la aplicación de la metodología como lo menciona (Guerrero Julio & Gómez Flórez, Gestión de riesgos y controles en sistemas de información: del aprendizaje a la transformación organizacional, 2012) “es de suma importancia para la toma de decisiones acertadas sobre las políticas y las estrategias de control relacionadas con sus vulnerabilidades.”

6.3 Identificación del Riesgo

Dentro de una organización, emplear gestión de riesgos es prácticamente el diagnóstico del negocio, identificar claramente los riesgos de los activos antes valorados. Esto conlleva la identificación, descripción y análisis de la situación actual de una organización, así como refiere (Postgrado, 2017) La identificación del riesgo “revisa la lista de posibles fuentes de riesgo, así como la experiencia y el conocimiento del personal dentro del área organizativa, se identifican todos los potenciales riesgos, los riesgos son categorizados y priorizados. El proceso de priorización ayuda a gestionar aquellos riesgos que tienen un alto impacto y una alta probabilidad de ocurrencia.”

6.4 Análisis del Riesgo

El análisis de riesgos es una herramienta que permite identificar, clasificar y valorar los eventos que puedan amenazar la consecución de los objetivos de la organización y establecer las medidas oportunas para reducir el impacto esperable hasta un nivel tolerable (ISO27005, 2008).

El objetivo del análisis y la gestión del riesgo no es la eliminación completa del riesgo, sino su reducción a unos niveles tolerables para la organización en función de su apetito al riesgo (Matalobos & Carrillo, 2009).

6.5 Evaluación del Riesgo

Diseñar escenarios en los cuales se posibilitaría la existencia de los riesgos. Esta actividad permite ponderar el impacto organizacional que cada uno de los escenarios tendría en los activos del negocio.

Por otro lado, de acuerdo con la perspectiva planteada por los estándares SP800-39, SP800-30, MEHARY e ISM3, el impacto generado por los riesgos es diferente pues depende de los escenarios organizacionales en que se presenten. Esto implica que las organizaciones deberán definir los niveles apropiados de riesgo teniendo en cuenta su naturaleza compleja, para posteriormente asociarlos con los escenarios en los cuales se podrían presentar (Guerrero Julio & Gomez Flores, Revisión de estándares relevantes y literatura de gestión de riesgos y controles en sistemas de información, 2011)

Para el establecimiento de criterios de evaluación de probabilidad, se sustenta en la Norma ISO/IEC 27005 definida en el proceso de estimación del riesgo. En esta actividad se definen medidas de probabilidad basados en la frecuencia de qué tan probable es que ocurran amenazas. El autor (USBMed, 2014) menciona las siguientes pautas para tomarse en cuenta en la evaluación de probabilidad:

- Los tipos de amenazas a los activos críticos
- Con qué frecuencia ha ocurrido cada amenaza en el pasado (la historia)

6.6 Tratamiento del Riesgo

En esta etapa se debe de seleccionar alternativas de mitigación que mejoren la seguridad de la organización mediante la reducción del riesgo (Arevalo M. , 2017).

Terminada la evaluación del riesgo, se ejecutan las medidas correctivas, se escoge una serie de opciones para mitigar el riesgo; este es un proceso repetitivo que tiene como fin determinar su tolerabilidad en contra de los criterios establecidos, con el fin de decidir si se requiere un tratamiento posterior. Los riesgos son monitoreados cuando superan los umbrales establecidos, los planes de mitigación de riesgos se despliegan para devolver el esfuerzo afectado a un nivel de riesgo aceptable. Si el riesgo no puede ser mitigado, se puede invocar un plan de contingencia (Vanegas , Gonzalo , & Pardo, 2014).

7. CAPITULO I DIAGNÓSTICO

Con el desarrollo de este capítulo se pretende cumplir con los objetivos [1], [2] y [3] contemplados dentro de la fase planeación del ciclo de Deming que tiene 4 fases bien definidas: Plan, Do, Check y Act (Planeación, Ejecución, Verificación y Actuación) soportada bajo la Norma ISO/IEC 27005 de gestión de riesgos tecnológicos en el Área de Base de Datos de la División de Informática y Sistemas de la DGI, donde se realizó la recolección de los datos (Este proceso se describe en la fase de 7.3.1 Evaluación de las consecuencias) para determinar qué los puede afectar a nivel interno y externo (**Diagnostico del Contexto**), qué requieren proteger y de acuerdo a los recursos actuales (físicos, tecnológicos y operativos) cómo podría darse esa protección (**Identificación de amenazas, vulnerabilidades y riesgos**) para establecer el nivel de aceptación de riesgo al cual están dispuestos (**Evaluación del riesgo**), determinar los alcances y limitaciones existentes para evaluar los posibles **planes de tratamiento de riesgos** que ayuden a la alta gerencia a la toma de decisiones.

Por tanto, la adaptación de la Norma ISO/IEC 27005 se define en la figura 3, la cual está contemplada hasta el proceso de Tratamiento del Riesgo.

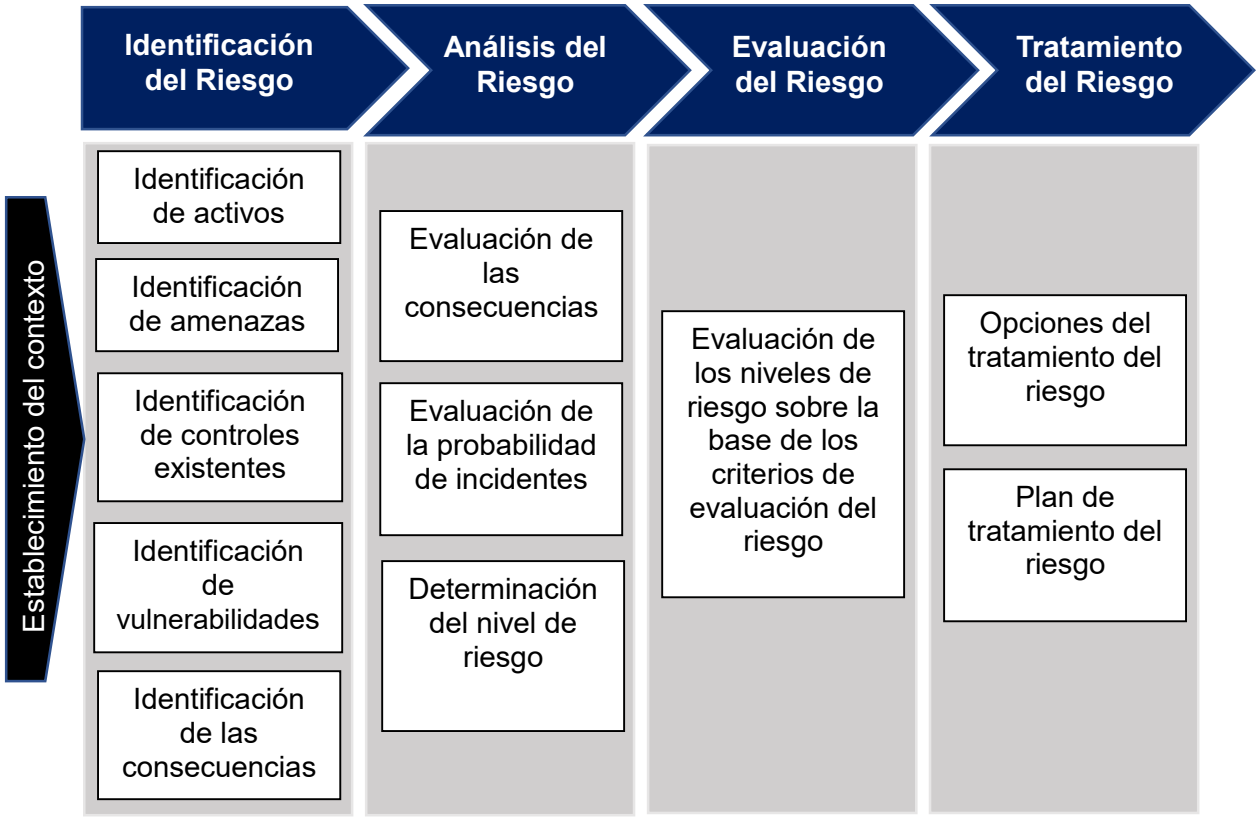


Ilustración 1 Alcance de la Norma ISO/IEC 27005

7.1 ESTABLECIMIENTO DEL CONTEXTO

Basado en la Norma ISO/IEC 27005 , el establecimiento del contexto se clasifica en: Contexto Interno (**Véase Anexo: Sección 5, Pág. 89**) y Contexto Externo (**Véase Anexo: Sección 5, Pág. 87**). En esta parte se define el alcance de la gestión del riesgo dentro del área de base de datos, se identifican las metas de la organización alineadas al área de TI, los objetivos del área de base datos para dar cumplimiento a las metas de la organización, responsabilidades, relación con los otros procesos, y todos los recursos o procesos que el área de base de datos considera críticos para obtener una apreciación del riesgo.

7.1.1 Contexto Interno

La Dirección General de Ingresos (DGI), es una institución descentralizada con autonomía administrativa y financiera, cuyo objeto es aplicar y hacer cumplir las leyes, actos y disposiciones que establecen o regulan ingresos a favor del estado, que están bajo la jurisdicción de la Administración Tributaria,

Visión

Ser una Administración Tributaria profesional, ágil y sencilla al servicio del pueblo nicaragüense.

Misión

Recaudar los tributos internos con equidad, transparencia y eficiencia, promoviendo la cultura Tributaria y cumpliendo con el Marco Legal, aportando al Gobierno recursos para el desarrollo económico y social del país.

La División de Informática y Sistemas que se encuentra dividida en:

- ✓ Área de Sistemas Tributarios
- ✓ Área de Control de Calidad
- ✓ Área de Apoyo Tecnológico

El área de Apoyo Tecnológico se encuentra distribuida en las siguientes divisiones específicas:

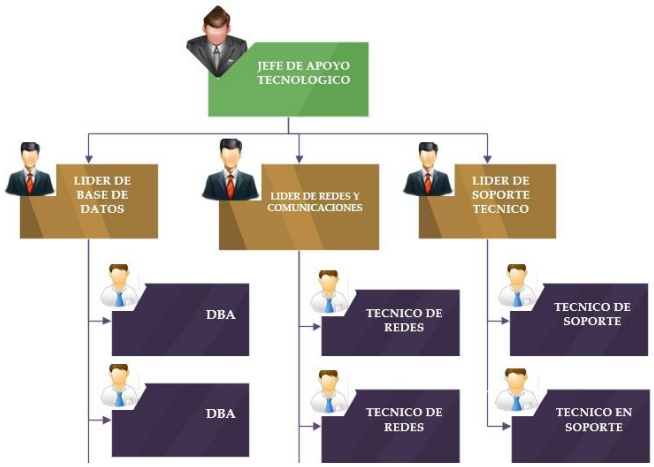


Ilustración 2 Organigrama de la División de Informática y Sistemas de la DGI

Los involucrados dentro del área de Bases de Datos y Sistemas Operativos:

Jefe de la Unidad de Apoyo Tecnológico: es el encargado de la Unidad de Apoyo Tecnológico a nivel general, el cual administra y ejecuta los requerimientos de más alto nivel y administra las 3 áreas a su cargo: UBSO, Comunicaciones y Redes y Soporte Técnico.

Líder de Bases de Datos y Sistemas Operativos: es el encargo de administrar el área específica de UBDSO además de distribuir de manera equitativa la ejecución de los requerimientos según un rol de rotación de servidores críticos y no críticos de la Dirección General de Ingresos.

Administradores de Bases de Datos: son el personal técnico encargado de ejecutar en tiempo y forma cada uno de los requerimientos solicitados y enviados por el Líder de Bases de Datos y Sistemas Operativos.

El área de Unidad de Bases de Datos y Sistemas Operativos (UBDSO), es la encargada de la ejecución de mantenimiento y administración de Bases de Datos, ejecución de sentencias en las Bases de Datos, mantenimiento y revisión de servidores en sistemas operativos Linux y Windows, brinda servicios y da soporte al resto de las áreas de TI, incluyendo las rentas administrativas de la Dirección General de Ingresos.

El área de base de datos tiene como objetivo hacer cumplir la misión de la organización: “Recaudar los tributos internos con equidad, transparencia y eficiencia”, mediante la disponibilidad e integridad de los servicios que permiten la recaudación en línea.

7.1.2 Contexto Externo

Tabla 4: Análisis FODA del área de Bases de Datos.

Fortalezas	Debilidades
• Buen ambiente laboral. • Pro actividad en la gestión de servicios. • Inversión en Tecnología	• Rotación del personal. • Falta de experiencia en el personal • Falta de motivación de los recursos humanos.
Oportunidades	**Amenazas**
• Fuerte poder adquisitivo del segmento meta (presupuesto tributario) • Mejora en la atención de sus clientes internos.	• Cambios en la legislación o leyes tributarias.

Podemos concluir que el proceso preliminar “establecimiento del contexto” cumple con el objetivo [1], permitiendo identificar el campo de estudio, la pertinencia de conocer y documentar el flujo de información que constituye la organización, es decir, entrada y salida de datos que el área de base de datos de TI realiza acorde a las metas establecidas para el cumplimiento de logros tributarios tomando en cuenta las variables que influyen tanto a nivel interno como externo, que afectan de una u otra forma en la toma de decisiones dentro de la gestión de riesgos.

7.2 IDENTIFICACIÓN DEL RIESGO

Esta fase según la Norma ISO/IEC 27005 se conoce como valoración de riesgos donde se identifican todos los riesgos potenciales dentro del Área de Base de Datos y Sistema Operativo que deberían aparecer en forma de escenarios identificando las posibles amenazas, vulnerabilidades y consecuencias relacionadas con los activos y procesos del área de base de datos para dar cumplimiento al objetivo [2]. El resultado es el “Catalogo de Riesgo”, comúnmente conocido como la lista de riesgos.

7.2.1 Identificación de activos

Para la identificación de los activos se debe tener en cuenta la fase preliminar "establecimiento del contexto", esta correlación permite valorar los posibles activos relevantes para Área de Base de Datos y Sistema Operativo incluyendo procesos, información, datos y activos de soporte que necesitan ser protegidos ya que estos afectan el proceso general y la determinación del contexto en particular dentro de la organización. La Norma ISO/IEC 27005 divide los activos en 2 categorías: Los activos principales (Activos Primarios) y Activos Secundarios (Activos de Apoyo). **Véase Anexo: Sección 6, Pág. 8**

2.2.1.1 Activos Primarios

A continuación, se presenta una lista de los activos principales (Activos Primarios) que se consideran en el área de Bases de Datos.

Tabla 5: Activos primarios del Área de Base de Datos y Sistema Operativo

Procesos	Descripción
Administración de permisos a las bases de datos	Asignación de privilegios a las BD según el perfil de usuario.
Administrar respaldos	Son las copias de seguridad de las BD más críticas almacenadas en distintos medios de almacenamiento
Publicación de sistemas	Publicación de sistemas de desarrollo a producción
Mantenimiento a las BD	Limpieza de Logs, de tablas, actualizaciones, etc
Servicios	El activo de servicios tiene por objeto satisfacer las necesidades de los usuarios, según los requerimientos que reportan al Área de Base de Datos y Sistema Operativo

2.2.1.2 Activos Secundarios

A continuación, se presenta una lista de los activos de apoyo (Activos secundarios) que se consideran en el área de Bases de Datos.

Tabla 6: Activos secundarios del Área de Base de Datos y Sistema Operativo

Categoría	Descripción	Herramientas de Apoyo
Hardware	Se refiere a bienes materiales que aportan el beneficio del soporte informático	Servidores, laptops, unidades de disco externo, etc.
Software	Todos los programas, aplicativos que contribuyen al tratamiento de datos	Sistemas operativos, programas de tratamiento de texto, gestores de base de datos
Redes	Todos los dispositivos de telecomunicaciones, utilizados para interconectar varios equipos o elementos físicamente remotos, de un sistema de información.	Router, firewall, cacle de red, llave, puente, etc.
Personal	Todas las personas involucradas en la manipulación de las BD.	DBA, Analista de Sistema y Control de Calidad.
Físico	Lugares físicos donde se llevan a cabo las operaciones.	Escritorio, Centro de Datos, oficinas
Estructura de la organización	Marco organizativo asignado para la realización de las actividades.	Organigrama institucional, proveedores.

7.2.2 Identificación de vulnerabilidad, amenaza, consecuencia y relación entre activos

Una vez identificado los activos principales en el Área de Base de Datos y Sistema Operativo, es importante reconocer los posibles campos de acción. Como primera opción se identificó las posibilidades de riesgo, qué área o proceso impactaría, qué lo causó y cuáles son sus efectos si llegase a materializarse.

Se creó un inventario de riesgos sobre la premisa del logro de los objetivos **Véase Tabla 4**. Se Analizó el riesgo desde sus orígenes, causa y posibles efectos para obtener la posibilidad de analizar los posibles escenarios de que un riesgo se materialice.

La matriz de riesgo (Activos Primarios) que se mostrara a continuación, está compuesta por los procesos que se realizan dentro del Área de Base de Datos y Sistema Operativo (columna 1), la descripción de las actividades que se derivan de ese proceso (columna 2), las posibles amenazas (columna 3), y vulnerabilidades (columna 4), para que un riesgo se materialice (columna 5).

Tabla 7:Matriz de riesgo (Activos Primarios)

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo
Administración de permisos a las bases de datos	Control de acceso o privilegio a las bases de datos	Divulgación de Información	Empleado insatisfecho	Pérdida de imagen, reputación, credibilidad, violación de la privacidad de los usuarios (Contribuyentes y personal de la institución).
		Ataques de SQL Injection a las BD	No activación de Firewall, uso de credenciales por default, datos sensibles sin cifrar	Hacking, desconfianza en la veracidad de la información de los contribuyentes, Perdida de imagen, reputación y credibilidad.
		Robo de información	Privilegios excesivos a BD	Divulgación de la Información, fraude, chantaje.
	Comprobación y monitoreo sobre las sentencias y programas que se ejecutan en las BD	Falla técnica	DBA no revisó el programa o sentencia a ejecutarse. Usualmente se da el caso cuando una analista por error olvidó cambiar el ip de desarrollo al de producción	Datos inconsistentes, pérdida de tiempo, perdida de información, retraso en las operaciones.

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo
	Monitoreo de la lista de procesos que se ejecutan en las bases de datos productivas.	Los sistemas que están de cara al contribuyente no estén disponibles en fecha límite para el pago de impuestos.	BD mal configurada, ejecución de consultas que superan el tiempo de respuesta del sistema, centro de cómputo sin ups	Interrupción de operaciones y servicios, clientes insatisfechos, pérdidas financieras.
Administrar respaldos	Copias de respaldos de servidores críticos a discos externos.	Corrupción de datos	Falta de respaldos de BD, o copias de seguridad incompleta.	Pérdida de datos, fraude, pérdida de reputación y credibilidad.
	Comprobación de datos íntegros sobre la elaboración de copias de seguridad.	Corrupción de datos	Falta de comprobación de copias de seguridad.	Perdida de datos, fraude, perdida de reputación y credibilidad.
	Elaboración de comprobantes sobre copias de seguridad de base de datos	Copia fraudulenta de BD	Almacenamiento no protegido, falta de autenticación y privilegios del usuario al servidor donde se realizan las copias de seguridad de la información	Robo de información, fraude, corrupción de datos.
Publicación de sistemas	Publicación de servicios en producción, previamente probados.	Disponibilidad de servicios	Desconocimiento técnico de la falla	Pérdida de disponibilidad del sistema

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo
	Control y seguimiento de los sistemas	Vencimiento de licencias	Falta de gestión y seguimiento de licencias en los equipos de cómputo.	Pérdida de imagen de la empresa, Hacking
Mantenimiento a las BD	Realización de actividades de mejoramiento en la bases de datos antes de fechas límites de pago (eliminación de logs, tablas temporales)	Ralentización de los servicios.	El administrador de base de datos olvide realizar el proceso	Pérdida de calidad del servicio
Servicios	Brindar respuesta en el menor tiempo posible a los requerimientos que solicitan los clientes internos.	Prioridad de requerimientos	Falta de conocimiento técnico	Retraso en los procesos.

La matriz de riesgo (Activos Secundarios) que se mostrara a continuación, está compuesta por los procesos que se realizan dentro del Área de Base de Datos y Sistema Operativo (columna 1), la descripción de las actividades que se derivan de ese proceso (columna 2), las posibles amenazas (columna 3), y vulnerabilidades (columna 4), para que un riesgo se materialice (columna 5).

Tabla 8: Matriz de riesgo (Activos Secundarios)

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo
Hardware	Mantenimiento de servidores (Espacios en disco, uso de memoria o cpu, recursos, etc.)	Falla técnica	Falta de monitoreo y revisión de servidores por parte del DBA	Interrupción en operaciones, pérdida de tiempo.
	Monitoreo de alarmas en centro de computo	Pérdida de servicios esenciales	Cambio de temperatura en los equipos de cómputo, puede recalentar los servidores y estos puedan quemarse, afectando directamente los ambientes alojados en los mismos.	falta de disponibilidad de un servicio.
Software	Monitoreo y reportes sobre fallas técnicas en el software	Mal funcionamiento del software	Software nuevo o inmaduro, daños de fábrica, software desactualizados, software mal instalado provocaría incompatibilidad con los sistemas alojados en ese servidor.	Ralentización de los servicios
	Actualización de versiones de software, gestores de BD y licencias	Falla técnica y presupuestos	Incompatibilidad entre el software y el servidor. Tecnología obsoleta y ocupa amplios recursos para ejecutar los sistemas productivos,	Al superar el límite de conexiones al servidor, se ralentizan los servicios.

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo
Redes	El DBA es responsable del monitoreo sobre los logs de errores en caso de problemas en los enlaces de red, entrada y salida de datos, se comunica al jefe de comunicaciones y se comprueban los servicios.	Falla técnica	Falta de identificación de algún problema por falta de experiencia.	Falta de disponibilidad de los servicios y de la información
Personal	Monitoreo y revisión de servidores y servicios de los sistemas productivos	Autenticación de credenciales débiles	Falta de políticas sobre credenciales.	Robo de credenciales
		Saturación de las BD	Insuficiente asignación de recursos respecto a la cantidad de información procesada.	Interrupción de las operaciones y de servicios
	Ejecución de requerimientos	Falla técnica	Falta de experiencia, Rotación de personal	Interrupción de las operaciones o caída de un servicio.

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo
Estructura de la organización	Las solicitudes de requerimientos de las diferentes áreas de TI y rentas administrativas de base de datos se realizan mediante correo.	Falta de cumplimiento sobre el proceso administrativo.	Ejecución de sentencias no autorizadas, publicación de sitios productivos no autorizados.	Falta de disponibilidad de los servicios.

Mediante la identificación del riesgo es posible determinar qué podría suceder que cause una pérdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida mediante la identificación vulnerabilidades, amenazas y riesgos potenciales en los activos más relevantes del Área de Base de Datos y Sistema Operativo.

7.3 ANALISIS DEL RIESGO

El análisis del riesgo implica desarrollar una comprensión del riesgo, para ello se hará una evaluación de las consecuencias por proceso, posteriormente se realizará una evaluación del riesgo donde se especificará el nivel de criticidad que tiene en base a las consecuencias encontradas. Esto proporciona elementos de entrada para la evaluación del riesgo y para tomar decisiones acerca de si es necesario tratar los riesgos, así como sobre las estrategias y los métodos de tratamiento del riesgo más apropiados, **Véase Anexo: Sección 7, Pág. 42**

7.3.1 Evaluación de las consecuencias

Para este proceso se tiene como dato de entrada las posibles consecuencias en la matriz de riesgo de cada activo mencionado en la Matriz de Riesgo **Tabla 4** y **Tabla 5**, posteriormente se evalúa el impacto y la probabilidad que estos riegos ocurran.

Para realizar la identificación del impacto y la probabilidad de los riesgos, se recolectaron fuentes de información y técnicas pertinentes, las cuales se mencionan a continuación:

- Registros anteriores
- Experiencia práctica y pertinente
- Entrevistas estructuradas
- Cuestionarios

La muestra recolectada en el área de base de datos y sistemas operativos de la dirección de informática y sistemas de la DGI, fue dirigida al Jefe inmediato del área para identificar los procesos que consideran clave y según su perspectiva como el personal que tiene a cargo realiza los procesos, asi mismo se recolectó información de las experiencias vividas por tres operarios y como se realizan los procesos a nivel operativo. **Véase Anexo 1,2,3 y 4.** El análisis de la recolección de datos fue realizado de forma cualitativo **Véase fase de tratamiento del riesgo** y cuantitativo **Véase fase de aplicación de análisis de resultado.**

Para los criterios de evaluación del riesgo por probabilidad, según la Norma ISO/IEC 27005 se muestra la siguiente escala:

Tabla 9: Escala de riesgo por probabilidad

Nivel	Escala Cualitativa	Descripción	Probabilidad
1	Improbable	Sucede ocasionalmente	Se presenta 1 vez de 3 a 5 años
2	Menos probable	Sucede en ciertos casos	Se presenta 1 vez de 2 a 3 años
3	Posible	Puede suceder	Se presenta cada 2 años en promedio
4	Muy posible	Sucederá en cualquier momento	Se presenta una vez al año en promedio
5	Casi seguro	Sucede en cualquier momento	Se presenta más de 1 vez cada 6 meses

Para los criterios de evaluación del riesgo por impacto, según la Norma ISO/IEC 27005 se muestra la siguiente escala:

Tabla 10: Escala de riesgo por impacto

Nivel	Escala Cualitativa	Descripción	Impacto
1	Insignificante	Perdidas mínimas	<10% de pérdidas anuales
2	Menor	Perdidas asumidas	>=10% <20% de pérdidas anuales
3	Moderado	Perdidas controladas	>=20% <30% de pérdidas anuales
4	Importante	Pérdidas significativas	>=30% - 70% de pérdidas anuales
5	Catastrófico	Presenta perdidas muy valiosas	>=70% de pérdidas anuales

El primer paso para evaluar las consecuencias del riesgo dentro del Área de Base de Datos y Sistema Operativo, se tomará en cuenta las escalas predefinidas anteriormente para determinar los niveles del activo, el nivel de la probabilidad de una amenaza, el nivel de las consecuencias para cada activo amenazado y posteriormente se calcula la medida

del riesgo multiplicando (probabilidad x impacto) = Medida del riesgo, véase la Tabla 11 valoración de riesgos.

7.3.2 Evaluación del riesgo

La evaluación del riesgo implica la comparación del nivel de riesgo hallado durante el proceso de análisis con los criterios de riesgo establecidos al considerar el contexto y posteriormente priorizarlos.

Para los criterios de evaluación de riesgos, se consideran los objetivos a cumplir dentro de la organización y dentro del Área de Base de Datos y Sistema Operativo, el contexto para la gestión de riesgos externos e internos y las opiniones de las partes interesadas.

Los criterios que se tiene en cuenta para la priorización de riesgos, se presentan a continuación:

Tabla 11: Escala para priorización de riesgos

Rango	Importancia
1 a 8	Baja
9 a 17	Media
18 a 25	Alta

A continuación, se mostrará la tabla de la valoración del riesgo tanto del contexto interno y externo del Área de Base de Datos y Sistema Operativo, evaluando por activo, la probabilidad, el impacto, determinación del nivel del riesgo y la clasificación de prioridad del riesgo.

Tabla 12: Valoración de los riesgos según la probabilidad y el impacto (Activos Primarios)

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Medida del riesgo	Prioridad del riesgo
Administración de permisos a las bases de datos	Control de acceso o privilegio a las bases de datos	Divulgación de Información	Empleado insatisfecho	Pérdida de imagen, reputación, credibilidad, violación de la privacidad de los usuarios (Contribuyentes y personal de la institución).	1	1	1	Baja
		Ataques de SQL Injection a las BD	No activación de Firewall, uso de credenciales por default, datos sensibles sin cifrar	Hacking, desconfianza en la veracidad de la información de los contribuyentes, Perdida de imagen, reputación y credibilidad.	4	3	12	Media
		Robo de información	Privilegios excesivos a BD	Divulgación de la Información,	4	4	16	Media

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Medida del riesgo	Prioridad del riesgo
				fraude, chantaje.				
	Comprobación y monitoreo sobre las sentencias y programas que se ejecutan en las BD	Falla técnica	DBA no reviso el programa o sentencia a ejecutarse. Usualmente se da el caso cuando una analista por error olvido cambiar el IP de desarrollo al de producción	Datos inconsistentes, pérdida de tiempo, perdida de información, retraso en las operaciones.	4	4	16	Media
	Monitoreo de la lista de procesos que se ejecutan en las bases de datos productivas.	Los sistemas que están de cara al contribuyente no estén disponibles en fecha límite para el pago de impuestos.	BD mal configurada, ejecución de consultas que superan el tiempo de respuesta del sistema,	Interrupción de operaciones y servicios, clientes insatisfechos, pérdidas financieras.	5	4	20	Alta

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Medida del riesgo	Prioridad del riesgo
Administrar respaldos	Copias de respaldos de servidores críticos a discos externos.	Corrupción de datos	Falta de respaldos de BD, o copias de seguridad incompleta.	Perdida de datos, fraude, perdida de reputación y credibilidad.	2	4	8	Baja
	Comprobación de datos íntegros sobre la elaboración de copias de seguridad.	Corrupción de datos	Falta de comprobación de copias de seguridad.	Perdida de datos, fraude, perdida de reputación y credibilidad.	5	4	20	Alta
	Elaboración de comprobantes sobre copias de seguridad de base de datos	Copia fraudulenta de BD	Almacenamiento no protegido, falta de autenticación y privilegios del usuario al servidor donde se realizan las copias de seguridad de la información	Robo de información, fraude, corrupción de datos.	1	4	4	Baja
Publicación de sistemas	Publicación de servicios en producción,	Disponibilidad de servicios	Desconocimiento técnico de la falla	Perdida de disponibilidad del sistema	4	4	16	Media

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Medida del riesgo	Prioridad del riesgo
	previamente probados.							
	Control y seguimiento de los sistemas	Vencimiento de licencias	Falta de gestión y seguimiento de licencias en los equipos de cómputo.	Pérdida de imagen de la empresa, Hacking	2	1	2	Baja
Mantenimiento a las BD	Realización de actividades de mejoramiento en la bases de datos antes de fechas límites de pago (eliminación de logs, tablas temporales)	Ralentización de los servicios.	El administrador de base de datos olvide realizar el proceso	Pérdida de calidad del servicio	4	3	12	Media
Servicios	Brindar respuesta en el menor tiempo posible a los	Prioridad de requerimientos	Falta de conocimiento técnico	Retraso en los procesos.	4	1	4	Baja

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Medida del riesgo	Prioridad del riesgo
	requerimientos que solicitan los clientes internos.							

A continuación, se mostrará la tabla de la valoración del riesgo tanto del contexto externo del Área de Base de Datos y Sistema Operativo, evaluando por activo, la probabilidad, el impacto, determinación del nivel del riesgo y la clasificación de prioridad del riesgo.

Tabla 13: Valoración de los riesgos según la probabilidad y el impacto (Activos Secundarios)

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Medida del riesgo	Prioridad del riesgo
Hardware	Mantenimiento de servidores (Espacios en disco, uso de memoria o cpu, recursos, etc.)	Falla técnica	Falta de monitoreo y revisión de servidores por parte del DBA	Interrupción en operaciones, pérdida de tiempo.	4	2	8	Baja
	Monitoreo de alarmas en centro de computo	Perdida de servicios	Cambio de temperatura en los equipos de cómputo,	falta de disponibilidad de un servicio.	1	1	1	Baja

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Medida del riesgo	Prioridad del riesgo
		esenciales	puede recalentar los servidores y estos puedan quemarse, afectando directamente los ambientes alojados en los mismos.					
Software	Monitoreo y reportes sobre fallas técnicas en el software	Mal funcionamiento del software	Software nuevo o inmaduro, daños de fábrica, software desactualizados, software mal instalado provocaría incompatibilidad con los sistemas alojados en ese servidor.	Ralentización de los servicios	2	1	2	Baja
	Actualización de versiones de software, gestores de BD y licencias	Falla técnica y presupuestos	Incompatibilidad entre el software y el servidor. Tecnología	Al superar el límite de conexiones al servidor, se	3	3	9	Media

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Medida del riesgo	Prioridad del riesgo
			obsoleta y ocupa amplios recursos para ejecutar los sistemas productivos,	ralentizan los servicios.				
Redes	El DBA es responsable del monitoreo sobre los logs de errores en caso de problemas en los enlaces de red, entrada y salida de datos, se comunica al jefe de comunicaciones y se comprueban los servicios.	Falla técnica	Falta de identificación de algún problema por falta de experiencia.	Falta de disponibilidad de los servicios y de la información	1	1	1	Baja
Personal	Monitoreo y revisión de servidores y servicios de	Autenticación de credenciales débiles	Falta de políticas sobre credenciales.	Robo de credenciales	4	1	4	Baja

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Medida del riesgo	Prioridad del riesgo
	los sistemas productivos	Saturación de las BD	Insuficiente asignación de recursos respecto a la cantidad de información procesada.	Interrupción de las operaciones y de servicios	4	4	4	Baja
	Ejecución de requerimientos	Falla técnica	Falta de experiencia, Rotación de personal	Interrupción de las operaciones o caída de un servicio.	1	1	1	Baja
Estructura de la organización	Las solicitudes de requerimientos de las diferentes áreas de TI y rentas administrativas de base de datos se realizan mediante correo.	Falta de cumplimiento sobre el proceso administrativo.	Ejecución de sentencias no autorizadas, publicación de sitios productivos no autorizados.	Falta de disponibilidad de los servicios.	2	1	2	Baja

7.3.3 Identificación de controles existentes

El Área de Base de Datos y Sistema Operativo, no cuenta con documentación de controles para la gestión de riesgos, sin embargo, en base a la lista de activos identificados anteriormente se recopiló información sobre los procesos actuales que realizan para el control de los mismos.

Actualmente la forma de identificar posibles riesgos, amenazas o vulnerabilidades es mediante tres ambientes de prueba en los sistemas (ASISTENCIA, DNAT, FISCALIZACION). Sin embargo, esto deja una gran brecha a posibles amenazas, vulnerabilidades y riesgos materializados, por lo que la mayoría de inconsistencias o riesgos materializados se tratan al momento de algún problema con dichos servidores, sistemas o base de datos reportados por los clientes internos. Una vez que se logra identificar el problema se realizan reuniones con las partes interesadas (Jefe de Apoyo Tecnológico y Dirección superior) para evaluar por criterios, qué tan grave es el riesgo y de qué forma se le puede dar tratamiento.

Otra de las formas que el Área de Base de Datos y Sistema Operativo implementa es que si ya se tiene planificado ejecutar algún proyecto de tecnología que refuerce la tecnología actual, este pasa por un proceso de licitación, para que los oferentes den sus ofertas y esto a su vez se evalúe con respecto al presupuesto destinado a tecnología.

Basado en lo anterior, la Norma ISO/IEC 27005 , se apoya a su vez de varias normas como la ISO/IEC 27002 que proporciona una lista de objetivos de control comúnmente aceptados y controles de las mejores prácticas para ser utilizadas como guía de aplicación al seleccionar y aplicar medidas de control para lograr la seguridad de la información dando cumplimiento al objetivo [3] del estudio (Estrada, 2006), (iso27000.es, 2013), (Ministerio de Tecnologías de la Información y las Comunicaciones). **Véase Anexo: Sección 9, Pág. 83**

Los controles identificados mediante los activos del Área de Base de Datos y Sistema Operativo se definen en la siguiente tabla.

Tabla 14: Controles de la norma ISO/IEC 27002 adaptados a los procesos del area de base de datos y sistema operativo

Controles ISO 270002	
A5	Política de seguridad de la información
A6	Organización de la seguridad de la información
A9	Control de acceso
A12	Seguridad de las operaciones
A14	Adquisición, desarrollo y mantenimiento de sistemas
A16	Gestión de Incidentes de seguridad de la información
A17	Aspectos de la seguridad de la información de la gestión de continuidad de negocio

Guiados por los controles de la norma ISO/IEC 27002, se pueden identificar los controles existentes en el área de Bases de Datos. **Véase Anexo: Sección 6, Pág. 25** Donde; M. A= Madurez actual, M. O= Madurez objetivo. **Véase Anexo: Sección 6, Pág. 26.** Los controles existentes se pueden evaluar en función de los niveles de madurez, como se definen en la siguiente tabla.

Tabla 15: Escala de nivel de madurez

Identificación del nivel de madurez	
0 Inexistente	Ausencia total de procesos identificables.
1 Inicial	Implantación de procesos caso por caso sin ningún método.
2 Repetible	No hay procesos estándar aplicados.
3 Definido	Los procesos están documentados y son comunicados.
4 Cuantificablemente Gestionado	Procesos supervisados y medidos.
5 Optimizado	Procesos Optimizados.

A continuación, se muestra una matriz con los controles que sugiere la norma ISO/IEC 27002 basado en los procesos más críticos que se ejecutan dentro del Área de Base de Datos y Sistema Operativo. Esta matriz contempla los dominios, los controles que deberían cumplirse según la norma, los controles existentes dentro del área de base de datos, la evaluación del estado actual (M.A) del control versus el estado objetivo (M.O) donde se quiere llegar, el análisis de brechas y el responsable de que se ejecute el control.

Tabla 16: Matriz de controles existentes en el área de base de datos vs controles recomendados por la norma ISO/IEC 27002

Control de Seguridad	Requisito	Descripción de la situación actual	M.A	M.O	Análisis de brechas	Responsable
A5. Políticas de seguridad de la información						
A5. 1 Documento de políticas para seguridad de la información	Realizar un documento que contenga políticas sobre la información almacenada en las Bases de Datos.	Existen políticas de seguridad de la información en el área de Bases de Datos pero no está documentada.	1	3	La comunicación con los empleados no está provista eficientemente.	Líder de Base de Datos y Sistema Operativo
A6. Organización de la seguridad de la información						
A6.1 Roles y responsabilidades para la seguridad de información	Aprobación de un documento donde se define y asigne todas las responsabilidades de la seguridad de la información en las bases de datos y servidores del área de Bases de Datos.	El documento se aprueba al momento de entregar los servidores que tendrá asignado cada DBA, pero hay deficiencia en el cumplimiento de las mismas por parte de los administradores de base de datos	3	4	Las políticas de asignación de responsabilidades no son revisadas, ni evaluadas por el líder de base de datos y sistema operativo.	Líder de Base de Datos y Sistema Operativo
A6.1.1 Políticas sobre el contacto con las Autoridades pertinentes por cada área	Conocer los contactos apropiados con las autoridades pertinentes, para la aprobación y ejecución de requerimientos que son solicitados al Área	Las políticas sobre el contacto con las autoridades pertinentes por cada área existe por muchos años, pero algunas veces no se	1	5	Revisión y aprobación de las políticas sobre el contacto con las autoridades pertinentes por cada área existe	Jefe de Apoyo Tecnológico

Control de Seguridad	Requisito	Descripción de la situación actual	M.A	M.O	Análisis de brechas	Responsable
	de Base de Datos y Sistema Operativo .	cumple en su totalidad.				
A9. Control de accesos						
A9.1 Política sobre el uso de los servicios de red	Se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente	Se tiene un control de acceso de usuarios mediante políticas de red y firewall, sin embargo no existe una revisión constante sobre el paso de servicios de red a usuarios específicos en los servidores asignados a cada administrador de base de datos.	1	5	Falta de revisión para el control de accesos de los usuarios.	Líder de base de datos y Administradores de base de datos.
A9.2 Suministro de acceso de usuarios	Proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas, Base de datos y servicios	La política existe pero no siempre se cumple, especialmente al momento de revocar los derechos de acceso a los usuarios.	3	5	Falta de comunicación entre los usuarios clientes (es decir, las áreas que requieran quitar privilegios aun usuario) y el área de base de datos, ya sea porque no está asignado a un sistema	Líder de base de datos y jefes de los clientes internos.

Control de Seguridad	Requisito	Descripción de la situación actual	M.A	M.O	Análisis de brechas	Responsable
					específico o bien porque ya no trabaja en el área.	
A9.2.1 Gestión de derechos de acceso privilegiado	Política que restrinja y controle la asignación y uso de derechos de acceso privilegiados en los servidores asignados a los administradores de base de datos (DBA)	La política existe hace varios años, sin embargo, muchas veces no se cumple, cada DBA debería tener un usuario asignado por servidor con privilegios restringidos por seguridad, sin embargo, la mayoría de estos ocupan usuarios privilegiados.	3	5	Revisión de política de restricción y acceso privilegiados a servidores	Líder de base de datos, administrador de base de datos.
A9.2.2 Revisión de los derechos de acceso de usuarios	Revisión de la política de los derechos de acceso de usuarios a las base de datos	La política no está documentada, pero se realiza de forma empírica, depende de la responsabilidad de cada DBA administrar correctamente sus servidores.	1	4	Los DBA encargados de cada servidor deberían revisar los derechos de acceso a los usuarios clientes a intervalos regulares.	Administrador de base de datos

Control de Seguridad	Requisito	Descripción de la situación actual	M.A	M.O	Análisis de brechas	Responsable
A9.2.3 Retiro o ajuste de los derechos de acceso	Documentación de los derechos de acceso de todos los empleados y de usuarios externos de la información y a las instalaciones de procesamiento de la información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían de ajustar cuando se hagan cambios.	No existe un documento formal sobre este control, sin embargo algunas veces se cumple mediante correo electrónico informando al área de base de datos la baja de algún empleado.	2	5	Falta de comunicación entre los jefes clientes internos y el área de base de datos para quitar el acceso a información, en los ambientes de prueba cuando un empleado ya no labora para la institución.	Líder de base de datos y jefes de clientes internos
A12 Seguridad de las operaciones						
A12.1 Procedimientos operacionales y responsabilidades	Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten	Por muchos años se ha fomentado la documentación de los procedimientos de operación dentro del área de base de datos, actualmente existe una plataforma para subir cualquier documentación, sin embargo esta información no se actualiza.	3	5	Falta de actualización de información sobre los procedimientos de operación dentro del área de base de datos.	Líder de base de datos

Control de Seguridad	Requisito	Descripción de la situación actual	M.A	M.O	Análisis de brechas	Responsable
A12.1.1 Gestión de capacidad	Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura	Actualmente no existe un proceso sobre pruebas de estrés en los servidores o sistemas para probar la capacidad que soportan, a menos que ocurra un incidente.	2	5	Elaborar documentación sobre los un proceso sobre pruebas de estrés en los servidores o sistemas para probar la capacidad que soportan.	Jefe de Apoyo Tecnológico, líder de base de datos
A12.1.2 Separación de los ambientes de desarrollo, pruebas y operación	Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	Existe una separación de los ambientes de desarrollo, prueba y operación, sin embargo, a veces un usuario puede tener los mismos privilegios en varios ambientes de pruebas, lo que algunas veces implican borrado de datos y esto afecta a los dueños de los demás ambientes de prueba.	1	5	Elaboración de política sobre la comunicación entre un jefe de un área a otra cuando requieren hacer cambios drásticos en ambientes de prueba, y comunicarlo al área de Bases de Datos	Jefes de clientes internos y líder de base de datos.
A12.2	Se deberían hacer copias de respaldo de la	Existe un sistema de control de respaldo	2	5	Comprobación de la veracidad e	Líder de base de datos y

Control de Seguridad	Requisito	Descripción de la situación actual	M.A	M.O	Análisis de brechas	Responsable
Respaldo de información	información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	de la información en el área de Bases de Datos, sin embargo, no existe un proceso para poner a prueba dicha información y verificar que los datos están correctos.			integridad de la información respaldada	administrador de Base de Datos
A12.3 Registro de eventos	Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información	No se realiza un control de eventos de la seguridad de la información, actualmente esto se da a conocer cuando un DBA notifica al líder de base de datos que ha cometido algún error deliberadamente en algún ambiente o base de datos.	0	4	Elaborar una política donde haya un seguimiento regular sobre los registros acerca de actividades del DBA, excepciones, fallas y eventos de seguridad de la información	Jefe de Apoyo Tecnológico, Líder de base de datos y sistema operativo.
A12.3.1 Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.	La política existe desde hace 6 años, sin embargo no todos los DBA lo realizan, tampoco se realiza una revisión periódica.	1	4	Revisión periódica sobre el cumplimiento de esta política.	Líder de base de datos.

Control de Seguridad	Requisito	Descripción de la situación actual	M.A	M.O	Análisis de brechas	Responsable
A14 Adquisición, desarrollo y mantenimiento de sistemas						
A14.1 Ambiente de desarrollo seguro	Revisión periódica sobre el monitoreo en ambientes de pruebas para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas..	Falta de coordinación entre el administrador de base de datos y el analista para el monitoreo de las pruebas.	1	5	No existe un documento definido para la gestión de pruebas en el área.	Líder de Base de Datos y Líder de Sistema Tributario
A16 Gestión de incidentes de seguridad de la información						
A16.1 Gestión de incidentes y mejoras en la seguridad de la información	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.	Existe una política de seguridad de la información que es revisada por la alta dirección y el jefe de apoyo tecnológico, pero el documento nunca se ha publicado para todos los DBA.	2	5	La publicación con los DBA y otras personas afectadas por ella no está provista eficientemente	Jefe de apoyo Tecnológico
A16.1.1 Reporte de debilidades de seguridad de la información	Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de	Actualmente existe una política de monitoreo sobre los servidores que tiene asignado cada DBA, sin embargo, no se realiza una constate revisión y monitoreo	2	4	Ineficiencia en el monitoreo regular de los servidores asignados a cada DBA	Administrador de base de datos y líder de apoyo tecnológico.

Control de Seguridad	Requisito	Descripción de la situación actual	M.A	M.O	Análisis de brechas	Responsable
	seguridad de la información observada o sospechada en los sistemas o servicios.	sobre los mismos donde se observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.				
A17. Gestión de continuidad del negocio						
Planificación de la continuidad de la seguridad de la información	La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, durante una crisis o desastre.	No existe un plan de continuidad para la seguridad de la información en el área de Base de Datos.	0	5	No está definida en la agenda una revisión anual de la continuidad para la seguridad de la información por la Dirección de la institución	Jefe de Apoyo Tecnológico
A18. Cumplimiento						
Protección de registros	Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de	Existen políticas de protección de los registros en las bases de datos, sin embargo no se da seguimiento de este proceso	1	5	Falta de documentación y revisión de las políticas de protección de los registros de las bases de datos.	Jefe de Apoyo Tecnológico

Control de Seguridad	Requisito	Descripción de la situación actual	M.A	M.O	Análisis de brechas	Responsable
	acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.					

En las tablas anteriores se puede observar que los controles existentes de los activos del Área de Base de Datos y Sistema Operativo pueden causar vulnerabilidades en cuanto a la situación en la que el control seleccionado (o la estrategia) falla en su funcionamiento y, por lo tanto, se requieren controles complementarios para tratar de manera eficaz el riesgo identificado y disminuir la ocurrencia de eventos asociados a riesgos tecnológicos en el Área de Base de Datos y Sistema Operativo de la Dirección de Informática y Sistemas de la DGI.

8. CAPÍTULO II PROPUESTA

Este proceso ha consiste en la realización de un análisis de riesgos de la seguridad de la información que permita cuantificar y comparar los requerimientos de seguridad de la información de la organización con controles implantados para su cumplimiento y en base a las diferencias encontradas definir los controles adicionales necesarios para cumplir todos los requerimientos.

8.1 TRATAMIENTO DEL RIESGO Y ACEPTACIÓN DEL RIESGO

Después de haber realizado la valoración del riesgo, es necesario planificar de qué manera se van a contrarrestar aquellos escenarios que dieron valores altos (no aceptables) mediante el tratamiento de los riesgos donde se implementan las acciones a tomar para mitigar los riesgos encontrados y lograr riesgos residuales aceptables por la organización para dar cumplimiento al objetivo [4] del estudio, dentro de las acciones a tomar encontramos principalmente:

Modificación del Riesgo: Presentar, retirar o modifica los controles de modo que el riesgo residual puede ser evaluado como aceptable.
Retención del Riesgo: La dirección decidió aceptar el nivel real del riesgo.
Evitar el Riesgo: Cancelación o modificación de una actividad o conjunto de actividades relacionadas con los riesgos
Compartir el Riesgo: Decisión de compartir riesgos con las partes externas: pólizas de seguros o tercerización.

Donde, M= Modificación del Riesgo, R= Retención del Riesgo, E= Evitar el Riesgo, C= Compartir el Riesgo

Estas opciones de tratamiento del riesgo permitieron evaluar el apetito al riesgo de los activos del Área de Base de Datos y Sistema Operativo, tomando como punto de partida el análisis y la evaluación del riesgo previamente consensuada y realizada a través de la recolección de las fuentes de información sobre los procesos principales del área, de qué

forma se realizan y de qué manera afecta a la organización y al área de base de datos tener consecuencias negativas sobre los riesgos encontrados, permitiendo a la alta dirección facilitar el proceso de toma de decisiones sobre qué hacer y como mitigar la mayor parte de riesgos.

8.1.1 Descripción de las Matriz de Resultados

Una vez que se decidió aceptar el riesgo y las opciones de tratamiento del riesgo, se realiza el plan de tratamiento de riesgos que define la Norma ISO/IEC 27005 que consiste en documentar la manera en que se implantarán las opciones del riesgo, las prioridades a ser secuenciadas, las acciones a tomar, los recursos a asignar y las responsabilidades a tomar. Estas actividades de la Norma ISO/IEC 27005 proporcionan el cómo, porqué y qué implantar para cada actividad de los procesos más críticos del área de base de datos mejorando el desempeño de TI y/o tratar de mitigar el riesgo al nivel más bajo que se pueda.

La matriz está compuesta por los procesos que se realizan dentro del Área de Base de Datos y Sistema Operativo (columna 1), la descripción de las actividades que se derivan de ese proceso (columna 2), las posibles amenazas (columna 3), y vulnerabilidades (columna 4), para que un riesgo se materialice (columna 5), la medida del riesgo que resulta de la multiplicación de una vulnerabilidad por una amenaza (columna 6), la prioridad que tiene el riesgo (columna 7), la opción de tratamiento aceptada (columna 8), el control para mitigar el riesgo (columna 9), los recursos que se necesitan (columna 10), el mantenimiento o requerimiento (columna 11), y los responsables (columna 12).

Tabla 17: Plan de tratamiento del riesgo sobre los activos con alta valoración de riesgos

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo	Medida del riesgo	Prioridad del riesgo	Opción de tratamiento	control	Recursos necesarios	Mantenimiento requerido / comentarios	Responsable
Administrar respaldos	Ccomprobación de datos íntegros sobre la elaboración de copias de seguridad	Corrupción de datos	Falta de comprobación de copias de seguridad	Pérdida de datos, fraude, perdida de reputación y credibilidad.	20	Alta	E	Realizar copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	Preparar ambiente para comprobación de respaldos	Comprobación periódica de la veracidad e integridad de la información respaldada	Administrador de base de datos
Administración de permisos y ejecución de consultas a	Monitoreo de la lista de procesos que se ejecutan en las bases de	Los sistemas que están de cara al contribuyente no	BD mal configurada, ejecución de consultas que superan el tiempo de	Interrupción de operaciones y servicios, clientes insatisfecho	20	Alta	M	Optimización de consultas en la bases de datos y mejora en la configuración	Pruebas de tiempo sobre consultas que se ejecutaran en producción	Revisiones periódicas de la configuración y ejecución	Administrador de Base de Datos

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo	Medida del riesgo	Prioridad del riesgo	Opción de tratamiento	control	Recursos necesarios	Mantenimiento requerido / comentarios	Responsable
las bases de datos	datos productivas.	estén disponibles en fecha límite para el pago de impuestos.	respuesta del sistema	s, pérdidas financieras.				de recursos (procesamiento y almacenamiento) en las bases de datos		de sentencias en las bases de datos.	
Administración de permisos y ejecución de consultas a las bases de datos	Control de acceso o privilegio a las bases de datos	Ataques de SQL Injection a las BD	No activación de Firewall, uso de credenciales por default, datos sensibles sin cifrar	Hacking, desconfianza en la veracidad de la información de los contribuyentes, Perdida de imagen, reputación y credibilidad.	12	Media	E	Configuración de firewall en las bases de datos y canales de enlace por sitios públicos, encriptación de información sensible.	Revisión de servicio del firewall en servidores importantes	Revisión de la configuración del firewall. Clasificación de información sensible para la encriptación de datos.	Administrador de Base de Datos
Administración de permisos y ejecución de consultas a las bases de datos	Control de acceso o privilegio a las bases de datos	Robo de información	Privilegios excesivos a BD	Divulgación de la Información, fraude, chantaje.	16	Media	E	Brindar credenciales según roles y funciones a los usuarios de las bases de datos.	Software de control de acceso, análisis de logs e informes gerenciales, control de acceso físico	Modificar o proponer políticas contractuales, legales y regulatorias.	Administrador de Base de Datos

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo	Medida del riesgo	Prioridad del riesgo	Opción de tratamiento	control	Recursos necesarios	Mantenimiento requerido / comentarios	Responsable
								Separar o independizar las funciones de los usuarios de los sistemas de información, con el fin de evitar la incompatibilidad entre las mismas, los fraudes y los errores ocasionados por accesos autorizados o no autorizados	y protección de datos.		
Administración de permisos y ejecución de consultas a	Comprobación y monitoreo sobre las sentencias y programas	Falla técnica	DBA no reviso el programa o sentencia a ejecutarse. Usualmente se da el caso	Datos inconsistentes, pérdida de tiempo, perdida de información,	16	Media	M	Procedimientos de iniciación, aprobación y documentación,	Documento formal	Cumplimiento y revisión de documento para la ejecución	Administrador de base de datos

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo	Medida del riesgo	Prioridad del riesgo	Opción de tratamiento	control	Recursos necesarios	Mantenimiento requerido / comentarios	Responsable
las bases de datos	que se ejecutan en las BD		cuando una analista por error olvido cambiar el ip de desarrollo al de producción	retraso en las operaciones.				procedimientos de catalogación y mantenimiento, intervención de los usuarios, procedimientos de prueba y supervisión efectiva.		de programas en producción	
Publicación de Sistemas	Publicación de servicios en producción, previamente probados.	Disponibilidad de servicios	Desconocimiento técnico de la falla	Perdida de disponibilidad del sistema	16	Media	E	Procedimiento de pruebas. Supervisión efectiva	Realizar las pruebas de subsistemas y las pruebas de integridad del sistema de información cuando se consolidan los módulos. Revisión periódica de las	Monitoreo después de la publicación de servicios.	Administrador de base de datos, área de desarrollo (programadores)

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo	Medida del riesgo	Prioridad del riesgo	Opción de tratamiento	control	Recursos necesarios	Mantenimiento requerido / comentarios	Responsable
									actividades desarrolladas por los programadores de software		
Mantenimiento a las BD	Realización de actividades de mejoramiento en la bases de datos antes de fechas límites de pago (eliminación de logs, tablas temporales)	Ralentización de los servicios. Obsolencia tecnológica	El administrador de base de datos olvide realizar el proceso Incompatibilidad de software	Pérdida de calidad del servicio Perdida de integridad, confiabilidad y ralentización de servicios	12	Media	M	Configuración de recursos del procesamiento y almacenamiento de las Bases de Datos. Mejoramiento en los recursos tecnológicos	Limpieza de logs, limpieza de tablas temporales, particionamiento de tablas históricas Actualización de software y hardware	Revisión y monitoreo periódico de los recursos disponibles en las bases de datos.	Administrador de Base de Datos
Software	Realización de actividades de mejoramient	Ralentización de los servicios.	El administrador de base de datos olvide	Pérdida de calidad del servicio	12	Media	M	Configuración de recursos del procesamiento y	Limpieza de logs, limpieza de tablas temporales,	Revisión y monitoreo periódico de los recursos	Administrador de Base de Datos

Proceso	Actividades	Amenaza	Vulnerabilidad	Riesgo	Medida del riesgo	Prioridad del riesgo	Opción de tratamiento	control	Recursos necesarios	Mantenimiento requerido / comentarios	Responsable
	o en la bases de datos antes de fechas límites de pago (eliminación de logs, tablas temporales)	Obsolencia tecnológica	realizar el proceso Incompatibilidad de software	Perdida de integridad, confiabilidad y ralentización de servicios				almacenamiento de las Bases de Datos. Mejoramiento en los recursos tecnológicos	particionamiento de tablas históricas Actualización de software y hardware	disponibles en las bases de datos.	

Después de analizar y medir el valor del riesgo, se pasa a la evaluación de éstos, donde se clasifican atendiendo a su valor y límite permisible, como se observa en la Tabla 8. Los riesgos clasificados como **Altos** son los que amenazan considerablemente el éxito del proyecto estratégico de la organización (más de un 10 %). Éstos deben ser reducidos o eliminados lo más rápido posible con acciones preventivas y correctivas.

Los clasificados como **Medios** afectan moderadamente el éxito del proyecto estratégico de la organización (entre un 4 y un 7 %), o sea, menor que las clasificaciones anteriores. Por tanto, son menos significativos que los anteriores, pero se deben combatir con menos apuros que éstos.

Los riesgos **Bajos** son poco significativos, pues afectan en menor proporción al éxito del proyecto estratégico de la organización (menor que el 4 %). Por tanto, pueden ser aceptados por la organización, aunque a los riesgos bajos hay que darle seguimiento.

8.1.2 Aplicación de análisis de resultado cuantitativo

A continuación, se muestra uno de los procesos clave de los activos analizados en el Área de Base de Datos y Sistema Operativo con prioridad **ALTA** (Valor Riego: 20) en la matriz del plan de tratamiento del riesgo. Ver tabla 14

Nombre del proceso: Administración de permisos y ejecución de consultas a las bases de datos.

Para ello, se describe la plantilla de aplicación de análisis de resultado cuantitativo según (Veiga, 2009):

- **Introducción:** referencia al proyecto del análisis de riesgos y a sus resultados.

- **Objetivo:** conjunto de salvaguardas a implantar.

- **Alcance:** definición del entorno de la Sociedad donde se van a implantar las distintas salvaguardas.

- **Relaciones con otros proyectos:**
    - Identificación de los proyectos o tareas que deben haberse finalizado antes del inicio del proyecto o de alguna de sus fases.

- **Responsabilidades:** asignación de funciones y responsabilidades para el plan de tratamiento del riesgo.

  Para la asignación de responsabilidades se tuvo en cuenta el modelo RACI
  R: Realiza
  A: Responsables
  C: Colabora
  I: Es informado

- **Presupuesto:** Estimación de los recursos necesarios para la ejecución de tratamiento del riesgo, teniendo en cuenta:
    - Costes de implantación: hardware, software, servicios, personal interno.
    - Costes de mantenimiento: hardware, software, servicios, personal interno.

INTRODUCCIÓN Y ANTECEDENTES	DESCRIPCIÓN	RESPONSABILIDADES
La problemática que usualmente ocurre en el Área de Base de Datos y Sistema Operativo, es que los sistemas que están de cara al contribuyente no estén disponibles en fecha límite para el pago de impuestos, lo cual produce suspensión en sus operaciones normales, trayendo como consecuencia retraso en los pagos de forma presencial y a través de la ventanilla electrónica Tributaria (VET).	Interrupción de operaciones y servicios, clientes insatisfechos, pérdidas financieras, BD mal configurada, ejecución de consultas que superan el tiempo de respuesta del sistema.	**Responsable**: Líder de base de datos **Encargado**: DBA **Consultado**: Desarrollador **Informado**: Jefe de apoyo tecnológico

OBJETIVOS	DEPENDENCIAS	PRESUPUESTO
Las acciones a tomar son: *Actualización de gestores de base de datos que incluyan soporte. *Optimización de consultas en las bases de datos y mejora en la configuración de recursos (procesamiento y almacenamiento) en las bases de datos y servidores. * Pruebas de caja blanca	Ninguna	

Recursos	Implantación	Mantenimiento
Hardware Slot de memoria y almacenamiento en servidores virtuales	5,596 USD	1185,00 USD por 5 años
Software Actualización de gestores de base de datos que incluyan soporte	17,500 USD	
Servicio mejora en la configuración de recursos (procesamiento y almacenamiento) en las bases de datos por la empresa Software AG	5,000 USD	
Factor humano Capacitaciones al	18,000 USD	

ALCANCE-ÁMBITO DE APLICACIÓN	FACTORES CLAVES DE ÉXITO
Las acciones a tomar se aplicaron en el área de base de datos al proceso Administración de permisos y ejecución de consultas a las bases de datos productivas, cumpliendo con el objetivo IV del presente documento.	*Continuidad de Servicios. *Integridad, disponibilidad de los datos para realizar pago de tributos. *Mayor ingreso de tributos con servicios eficientes las 24 horas del día.

		personal encargado de los servidores productivos			
		Total	46,096 USD	1185,00 USD	

Tabla 18 Matriz de análisis cuantitativo

Es responsabilidad de los directores de la organización decidir el equilibrio entre los costos de la implementación de los controles y la asignación de presupuesto para dar cumplimiento a los objetivos del negocio, aunque estos excedan en factores de costo es conveniente tener en cuenta la seguridad de la información. Es por ello que la Dirección General de Ingresos ha explotado sus recursos en inversión tecnológica para dar un mejor servicio y atención a los usuarios para el pago de tributos visionando sus procesos a normas estandarizadas.

Inversiones en recurso humano por la Dirección General de Ingresos

Recientemente ha iniciado dicho proyecto que incluye 5 capacitaciones en estándares como (Norma ISO/IEC 27005 :2011 Gestión de Riesgo, COBIT 5, Desarrollo de Software seguros, Respuestas a incidentes de seguridad, norma ISO/IEC 22301:2012 Continuidad de operaciones) con una inversión aproximada de 118,000 euros, esto le permite expandirse a nuevas oportunidades de crecimiento en todos sus procesos.

8.2 EVALUACIÓN DEL RIESGO RESIDUAL.

El riesgo residual. Es el riesgo que permanece después que el riesgo ha sido tratado. **Véase Anexo: Sección 9, Pág. 99.** La norma ISO/IEC27005 define una escala del Valor de Control en base a nivel de criticidad del riesgo:

Tabla 19: Escala de valor de riesgo residual

Escala	Valor Control
Insignificante	0
Bajo	1
Medio	2
Alto	3
Muy alto	4

Para calcular el valor del riesgo residual se utilizó la fórmula de la Norma ISO/IEC 27005 :

VRR = VR – VC

VRR= Valor del Riesgo Residual

VR= Valor del Riesgo

VC= Valor Control

Se debe tener en cuenta que el riesgo residual es difícil de calcular, ya que según como se haya aplicado el control en el marco del tratamiento del riesgo, se le da un valor consensuado, evaluando que tanto se mitigo el riesgo y en base a ellos proceder a realizar los cálculos. Cabe mencionar que este proceso no se aplicó en el estudio, así como los últimos tres procesos que describe la norma para completar el ciclo de gestión de riesgos tecnológicos, ya que al principio de este estudio se definió el alcance de la aplicación de la norma hasta el proceso de Tratamiento del Riesgo, sin embargo se describirán a continuación para comprender la importancia que tienen los involucrados durante el proceso de la gestión de riesgos y como esta se debe de enriquecer cada día, mediante la mejora continua de los procesos que se mencionan en el desarrollo del todo el documento .

8.3 ACEPTACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

Esta fase tiene como fin tomar decisiones encaminadas a definir la responsabilidad de ser aceptados por la dirección; para cumplir con este requisito de la norma es necesario documentar los planes para el tratamiento del riesgo que deben describir la forma de valoración, con el fin de satisfacer los criterios de aceptación del riesgo antes definidos. De igual forma, es pertinente que la alta gerencia revise y apruebe los planes propuestos para el tratamiento del riesgo, los cuales se desarrollan y proyectan por especialistas en seguridad de la información. Aquí la premisa fundamental consiste en aceptar los riegos porque los beneficios que los acompañan son muy atractivos o porque el costo de la reducción del riesgo es demasiado alto.

8.4 COMUNICACIÓN DE LOS RIESGOS

La información producida en el proceso de gestión del riesgo se debe intercambiar y compartir con los responsables por activo, quienes toman decisiones respecto a acuerdos en la forma de gestionarlos.

En segunda instancia, la dirección toma la decisión final y aprueba la política general y específica, la norma vislumbra que la comunicación del riesgo se realiza para lograr proporcionar seguridad de la gestión del riesgo, recolectar información, compartir los resultados de la valoración del riesgo y presentar el plan para el tratamiento del riesgo esto para evitar o reducir la posibilidad de ocurrencia y el nivel de impacto de las brechas de seguridad.

Habría que decir también que para reducir las consecuencias de cualquier incidente la comunicación eficaz proporciona a directivos y partes involucradas un sentido de responsabilidad sobre el manejo de riesgos para mejorar la toma de conciencia al interior de la organización ante situaciones de emergencia y contribuir con el entendimiento del proceso en diversos niveles.

8.5 MONITOREO Y REVISIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

Los riesgos deben ser monitoreados y revisados con el fin de identificar cambios en la organización durante una etapa temprana para mantener la visión general y completa de los riesgos, teniendo en cuenta que no son estáticos sino cambiantes, es ineludible efectuar monitoreo constante para detectarlos y mitigar su impacto.

Este proceso ejerce control sobre: activos nuevos que se han incluido en el alcance de la gestión del riesgo, modificaciones sobre los activos de información, nuevas amenazas, vulnerabilidades que no han sido valoradas, impacto en las consecuencias de las amenazas evaluadas, incidentes y siniestros de seguridad. “Los riesgos requieren de un control iterativo y periódico que garantice las circunstancias cambiantes no alteren la criticidad de los riesgos.” Por tanto, el monitoreo y revisión es esencial e integral porque de ahí dependerá la alineación continua con el sistema de gestión.

Podemos resumir la metodología de la Norma ISO/IEC 27005 en cinco pasos esenciales, donde se obtienen información precisa para la adaptación de la misma en cualquier organización brindando las pautas necesarias para la gestión de riesgos tecnológicos asi como se muestra en la figura 5.

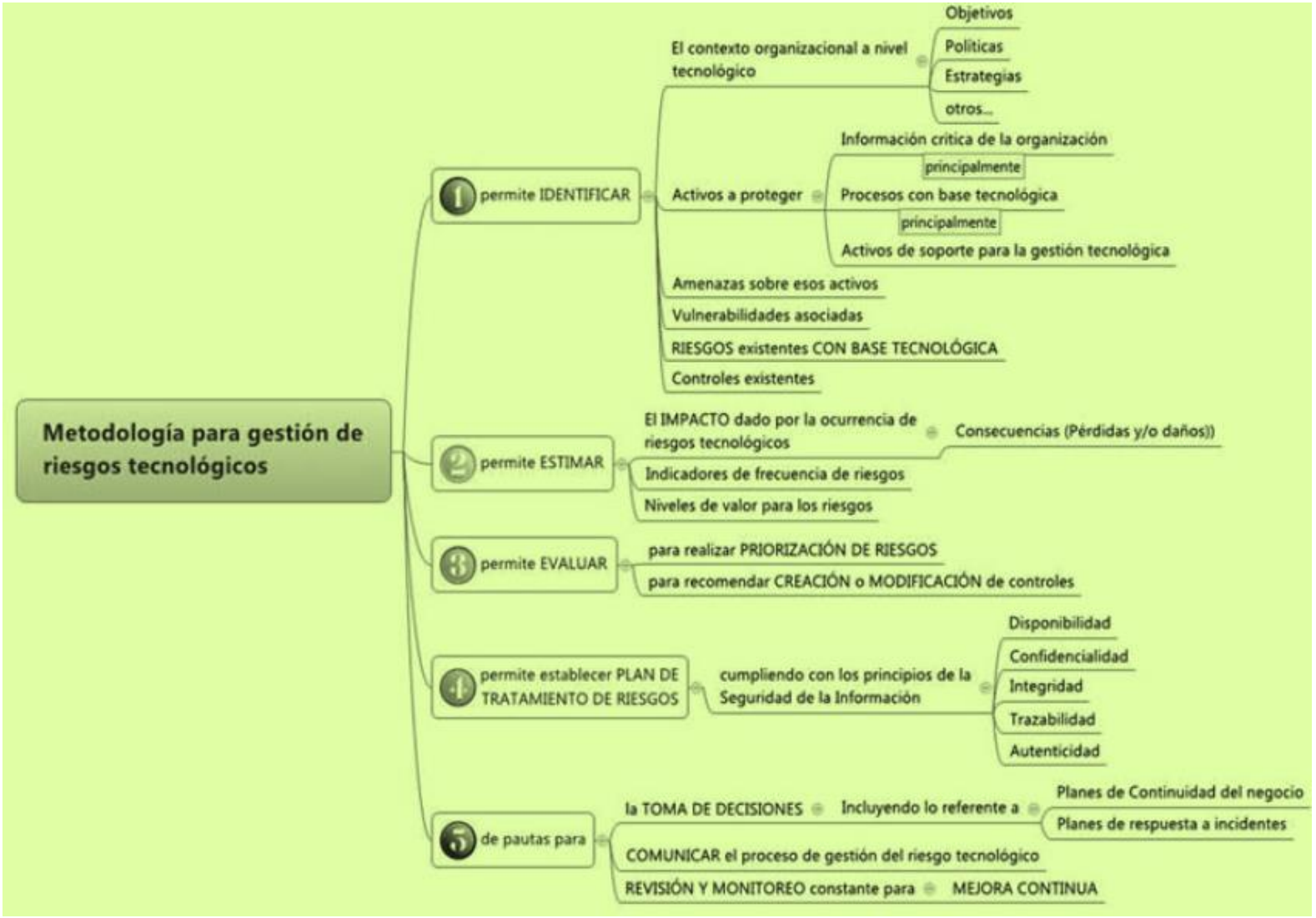


Ilustración 3 Pasos de la metodología para la gestión de gestión de riesgos noma ISO/IEC 27005

9 CONCLUSIONES

La gestión de riesgos es un factor fundamental para la implementación de seguridad de la información, debido a que permiten desarrollar estrategias para la mitigación de riesgos y ayudan crear conciencia en seguridad de la información para prevenir riesgos y obtener el apoyo de la alta gerencia con el fin de cumplir los objetivos y asegurar la información crítica mediante el alcance del contexto organizacional, es por ello que la “Aplicación de Gestión de Riesgos Tecnológicos basada en la norma ISO/IEC 27005 en el área de Base de Datos y Sistema Operativo de la Dirección de Informática y Sistemas de la DGI” robustece la protección de sus activos a nivel físico (lo correspondiente a infraestructura, incluyendo la tecnológica), nivel lógico (sistemas de información y software) y factor humano (toma de medidas organizacionales); en estos tres aspectos está presente el uso de tecnología y por ello la exposición a este tipo específico de riesgo crece constantemente.

La motivación de la norma ISO/IEC 27005 aplicada, proporciona lineamientos sobre cómo gestionar los riesgos por escenarios, enfoca los procesos, activos, amenazas y vulnerabilidades en un análisis de riesgo efectivo que optimiza el tiempo de ejecución y el aprovechamiento de recursos, evitando la reprocesamiento de actividades debido a la duplicidad de amenazas y controles; de igual forma permite plantear planes de remediación globales frente a escenarios de riesgo.

Finalmente se desarrolló el plan de tratamiento del riesgo que consta de una política de seguridad y un plan de ejecución que conlleva la participación del personal influyente sobre los activos principales del Área de Base de Datos y Sistema Operativo permitiendo la mejora de procesos aplicando medidas preventivas y correctoras para reducir los niveles de riesgo existentes.

10 RECOMENDACIONES

Los resultados obtenidos ayudarán a la organización a reconocer la necesidad de iniciar a implementar un plan de tratamiento de riesgo en el que se considere la contratación de personal especializado en seguridad, análisis de documentos y registros de incidentes, resultados de entrevistas al personal, para explotar la iniciativa del plan de tratamiento descrito en estudio “Aplicación de Gestión de Riesgos Tecnológicos basada en la norma ISO/IEC 27005 en el área de Base de Datos y Sistema Operativo de la Dirección de Informática y Sistemas de la DGI”.

Entre los lineamientos de futuros trabajos a desarrollarse se debería considerar desarrollar un análisis de riesgos de tipo cuantitativo considerando varios aspectos, como son: las consecuencias económicas de la materialización de una amenaza en cada activo, el costo del despliegue y mantenimiento de las salvaguardas; y estimar la probabilidad de ocurrencia de amenazas basándose en registros reales. También considerar los períodos de tiempo de recuperación de los procesos antes que las pérdidas se conviertan en irreparables y un análisis de aplicaciones críticas para definir prioridades de procesos.

11 GLOSARIO DE TÉRMINOS

La Norma ISO/IEC 27005 (Blog especializado en Sistemas de Gestión, 2017) fue publicada por primera vez en junio de 2008 y existe una versión mejorada del año 2011. Los siguientes términos y definiciones que se encuentran en el presente documento están Basados en la Norma NTC-ISO/IEC 27005.

Aceptación de riesgo: Decisión informada de asumir un riesgo concreto.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

Análisis de riesgos cuantitativo: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Confiabilidad de la Información: Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. La información debe ser accedida sólo por aquellas personas que lo requieran como una necesidad legítima para

la realización de sus funciones.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Impacto: El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros: pérdida de reputación, implicaciones legales, etc.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa

de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Propiedad de la información relativa a su exactitud y completitud. La información de la Superintendencia Nacional de Salud debe ser clara y completa, y solo podrá ser modificada por el personal expresamente autorizado para ello. La falta de integridad de la información puede exponer a la empresa a toma de decisiones incorrectas, lo cual puede ocasionar pérdida de imagen o pérdidas económicas.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Probabilidad: Medida para estimar la ocurrencia del riesgo.

Propietario del riesgo: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

Recursos de tratamiento de la información: Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo.

Selección de controles: Proceso de elección de las salvaguardas que aseguren la

reducción de los riesgos a un nivel aceptable.

SGSI: Sistema de Gestión de la Seguridad de la Información;

Sistema de Gestión de la Seguridad de la Información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

12 BIBLIOGRAFIA

Arevalo, M. (Agosto de 2017). Metodología Ágil para la Gestión de Riesgos Informáticos. *Killkana Técnica*, 31-42. Obtenido de http://killkana.ucacue.edu.ec/index.php/killkana_tecnico/article/view/81/122

Breier, J. (2014). *Asset Valuation Method for Dependent Entities.* Obtenido de https://dr.ntu.edu.sg/handle/10220/42540

Castro, R. (2011). Ingenieria. *Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios*, 56-66.

Diego Espinosa, Juan Martínez, Siler Amador. (2014). Gestión del riesgo en la seguridad de la información con base en la norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la metodologia OCTAVE-S. *Gestión del riesgo en la seguridad de la información con base en la norma*, Vol. 5, No. 2, pp. 33-43.

Estrada, A. C. (2006). ISO-27001: Los Controles (Parte II). *ISO-27001: Los Controles (Parte II)*, 1-17.

Franco, C. (2009). Graves problemas en la gestión de riesgo de las compañías. *Tendencias 21*.

García Porras, J., Huamani Pastor, S., & Lomparte Alvarado, R. (2018). Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas. *Revista Peruana de Computación y Sistemas*, 47-56. Obtenido de http://revistasinvestigacion.unmsm.edu.pe/index.php/rpcsis/article/view/14856/13008

Guerrero Julio, M., & Gomez Flores, L. (03 de Octubre de 2011). Revisión de estándares relevantes y literatura de gestión de riesgos y controles en sistemas de información. *Estudios Gerenciales*. Obtenido de https://ac.els-cdn.com/S0123592311701887/1-s2.0-S0123592311701887-main.pdf?_tid=24eab8a3-7d87-4b65-8a1f-2dc956b2a8cb&acdnat=1548315847_db59be78b8382ab879cf370c00e823ac

Guerrero Julio, M., & Gomez Flores, L. (03 de Octubre de 2011). Revisión de estándares relevantes y literatura de gestión de riesgos y controles en sistemas de información. *Estudios Gerenciales*. Obtenido de https://ac.els-cdn.com/S0123592311701887/1-s2.0-S0123592311701887-main.pdf?_tid=24eab8a3-7d87-4b65-8a1f-2dc956b2a8cb&acdnat=1548315847_db59be78b8382ab879cf370c00e823ac

Guerrero Julio, M., & Gómez Flórez, L. (2012). Gestión de riesgos y controles en sistemas de información: del aprendizaje a la transformación organizacional. *Estudios Gerenciales*, 87-95. Obtenido de https://www.sciencedirect.com/science/article/pii/S0123592312700116

Instituto Nacional de Ciber Seguridad. (s.f.). *Gestión de riesgos, una guia de aproximación para el empresario*. Obtenido de https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf

International Estandar ISO/IEC 27005. (2018). *Information technology-Security techniques-Information security risk management*. (I. 2018, Editor) Obtenido de www.iso.org

ISO 27000.ES. (s.f.). *El portal de ISO 27001 en Español*. Obtenido de

http://www.iso27000.es/iso27000.html

ISO 9001:2015. (8 de Noviembre de 2016). *Similitudes y diferencias en la gestión de riesgos en las normas ISO 9001, ISO 31000 e ISO 27001*. Obtenido de https://www.nueva-iso-9001-2015.com/2016/11/gestion-riesgos-iso-9001-iso-31000-iso-27001/

iso27000.es. (Octubre de 2013). *ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES* . Obtenido de http://iso27000.es/download/ControlesISO27002-2013.pdf

ISO27005. (2008). Obtenido de http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

ISOTools. (5 de Octubre de 2015). *Cómo implantar eficazmente la norma ISO 27005*. Obtenido de https://www.isotools.org/2015/10/05/como-implantar-eficazmente-la-norma-iso-27005/

ISOTools. (11 de Junio de 2017). *Gestión de Riesgos: diferencias entre ISO 31000 e ISO 27001*. Obtenido de https://www.isotools.org/2017/06/11/gestion-de-riesgos-diferencias-entre-iso-31000-e-iso-27001/

Kosutic, D. (s.f.). *Diferencias y similitudes entre ISO 27001 e ISO 27002*. Obtenido de https://advisera.com/27001academy/es/knowledgebase/diferencias-y-similitudes-entre-iso-27001-e-iso-27002/

Matalobos, J., & Carrillo, J. (Mayo de 2009). *Analisis de Riesgos de la Seguridad de la Información.* Obtenido de http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

Postgrado, G. E. (28 de Diciembre de 2017). *Gestión de riesgos: ¿Qué es? ¿Por qué emplearla? ¿Cómo emplearla?* Obtenido de https://gerens.pe/blog/gestion-riesgo-que-por-que-como/

Shanthamurthy, D. (Junio de 2011). *Leveraging ISO 27005 standard's risk assessment capabilities*. Obtenido de https://www.computerweekly.com/tip/Leveraging-ISO-27005-standards-risk-assessment-capabilities

Surridge, M., Bassem , N., Xiaoyu, C., Ajay , C., & Panos, M. (s.f.). *Run-Time Risk Management in Adaptive ICT Systems* . Obtenido de https://eprints.soton.ac.uk/370577/1/370577.pdf

USBMed, I. (Diciembre de 2014). Gestión del riesgo en la seguridad de la información con base en la norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la metodología OCTAVE-S. Obtenido de http://www.revistas.usb.edu.co/index.php/IngUSBmed/article/view/309/220

Vanegas , D., Gonzalo , A., & Pardo, C. (2014). Hacia un modelo para la gestión de riesgos de TI en en MiPyMEs: MOGRIT. *12*(30), 35-48. Obtenido de https://www.redalyc.org/pdf/4115/411534000003.pdf

Veiga, J. M. (Mayo de 2009). *Analisis de riesgo de seguridad de la informacion.* Obtenido de http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

ANEXOS

Anexo 1: Cuestionario

1. ¿Se tiene identificado los procesos claves dentro del área de base de datos que permiten a la organización cumplir con su misión?
2. ¿Cuál es el objetivo del proceso y subprocesos del área de base de datos?
3. ¿Cuál es el alcance del proceso y subprocesos del área de base de datos?
4. Mencione cuáles son las actividades que se relacionan con cada uno de los procesos antes mencionados.
5. ¿El área de base de datos actualmente funciona cuenta con políticas establecidas?, en caso afirmativo por favor mencionarlas.
6. ¿Cuenta con documentación donde se relacionen las actividades y responsabilidades de los procesos y subprocesos del área de base de datos? Si su respuesta es afirmativa, por favor facilitar la información.
7. ¿Cuáles son los riesgos a los que están expuestos durante la operación de los procesos y subprocesos del área de base de datos?
8. ¿Cuál es el impacto que se genera en las actividades críticas del área de base de datos?
9. ¿Cómo garantizan la continuidad del negocio en cuanto a herramientas tecnológica se refiere?
10. ¿Existen métodos de toma de información manuales en caso de que las herramientas tecnológicas fallen para el registro de incidentes?
11. ¿Cuál es el nivel de incidentes generados que puede causar un riesgo materializado?

Anexo 2: Formato para identificación de riesgos

Tabla para listar actividades y analizar causas de riesgos

No	Procesos	Subprocesos	Actividades	Causa del Riesgo	Riesgo
1					
2					
3					
4					

Anexo 3: Formato para evaluación de riesgos

Tabla para Evaluación de Riesgos

No	Procesos	Subprocesos	Actividades	Causa del Riesgo	Riesgo	Probabilidad	Impacto	Calificación	Valoración
1									
2									
3									
4									

Anexo 4: Formato para definición de tratamiento de riesgos

Tabla para evaluar riesgos

No	Procesos	Subprocesos	Actividades	Causa del Riesgo	Riesgo	Valoración	Tratamiento
1							
2							
3							
4							

En el siguiente gráfico, se muestran los procesos que integran la Norma ISO/IEC 27005 (International Estandar ISO/IEC 27005, 2018)

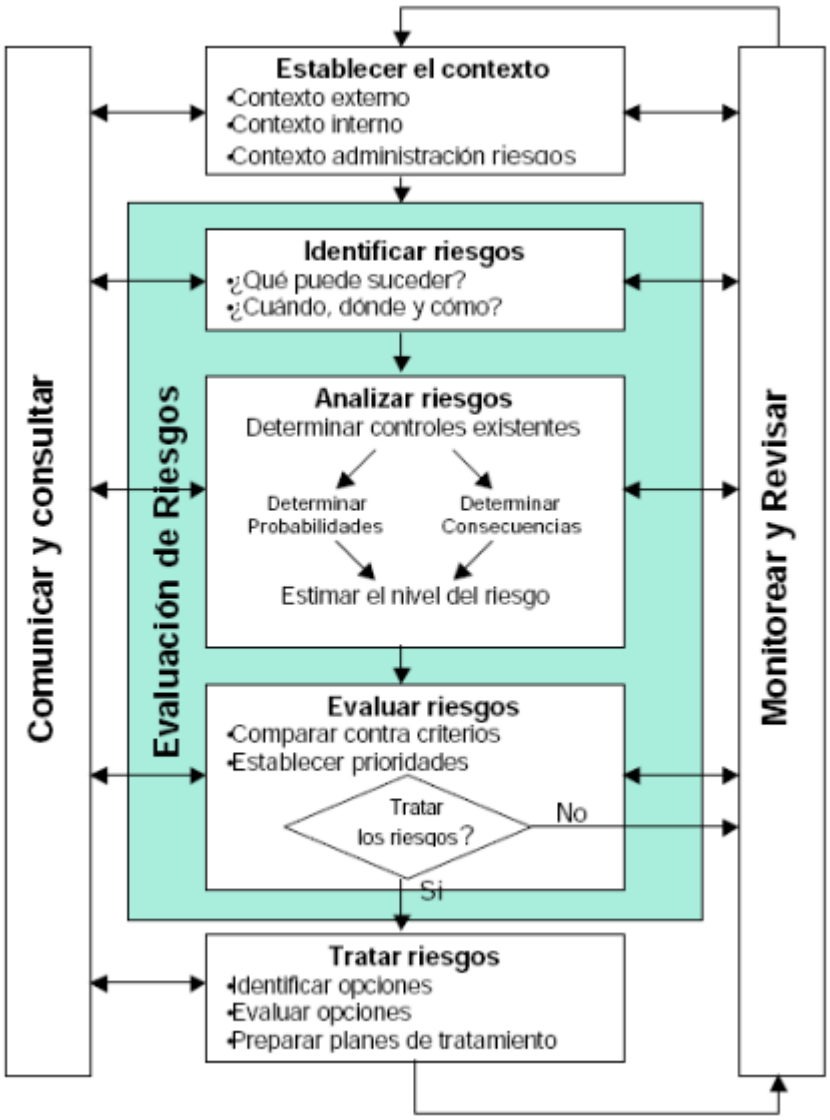
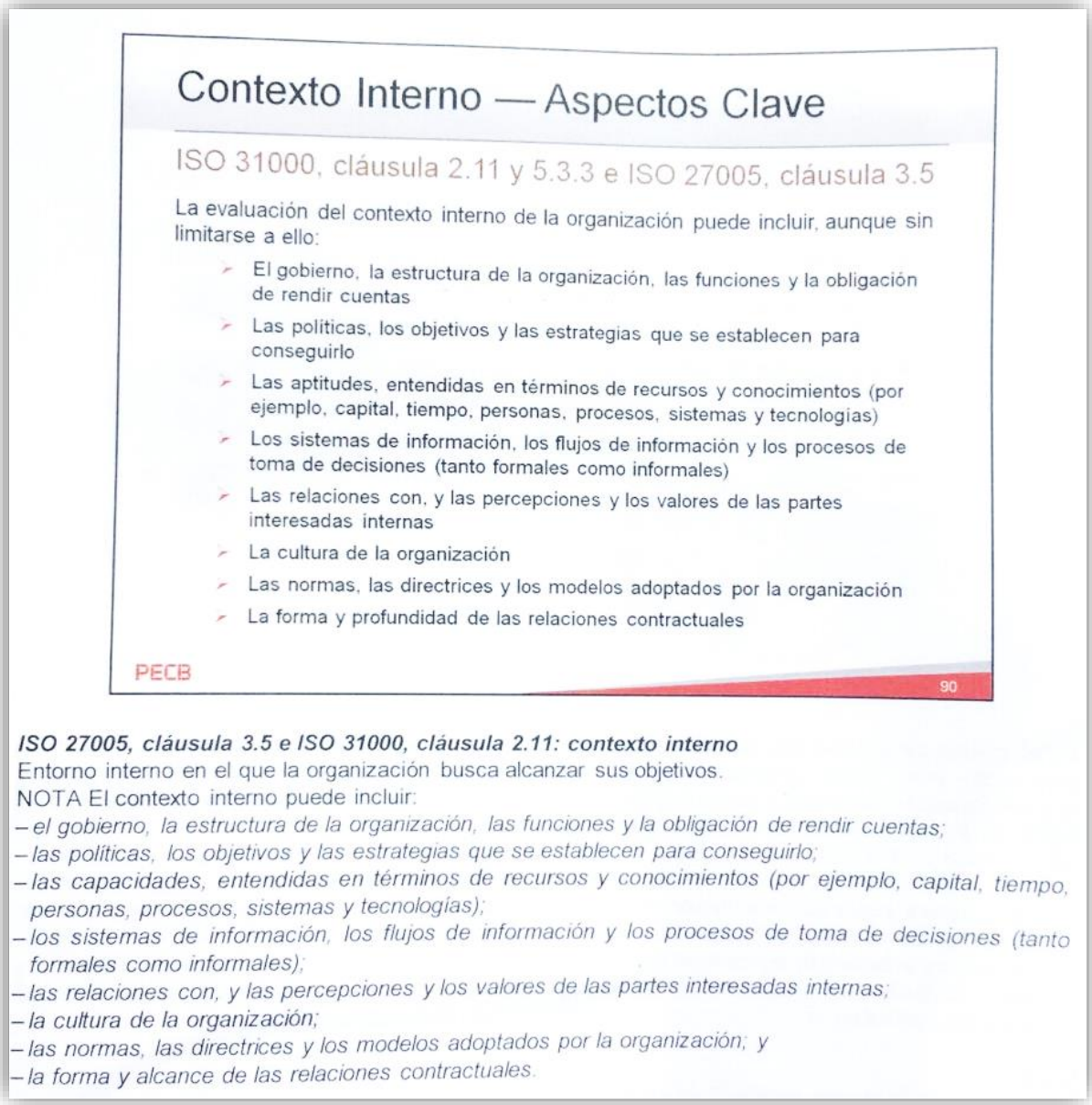


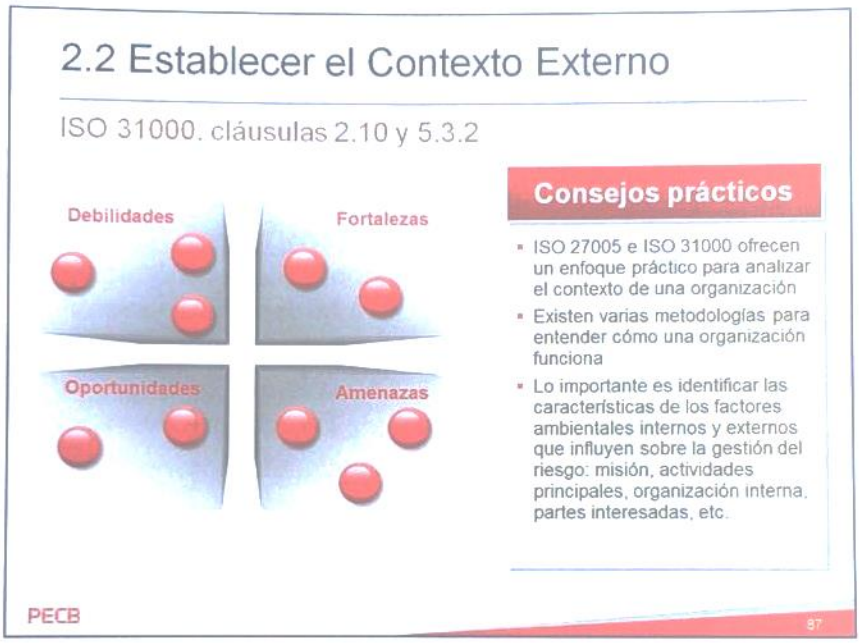
Ilustración 4 Norma ISO/IEC 27005

Anexo de libro: Sección 5, Pág. 89



ISO 27005, cláusula 3.5 e ISO 31000, cláusula 2.11: contexto interno
Entorno interno en el que la organización busca alcanzar sus objetivos.
NOTA El contexto interno puede incluir:
– *el gobierno, la estructura de la organización, las funciones y la obligación de rendir cuentas;*
– *las políticas, los objetivos y las estrategias que se establecen para conseguirlo;*
– *las capacidades, entendidas en términos de recursos y conocimientos (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías);*
– *los sistemas de información, los flujos de información y los procesos de toma de decisiones (tanto formales como informales);*
– *las relaciones con, y las percepciones y los valores de las partes interesadas internas;*
– *la cultura de la organización;*
– *las normas, las directrices y los modelos adoptados por la organización; y*
– *la forma y alcance de las relaciones contractuales.*

Anexo de libro: Sección 5, Pág. 87



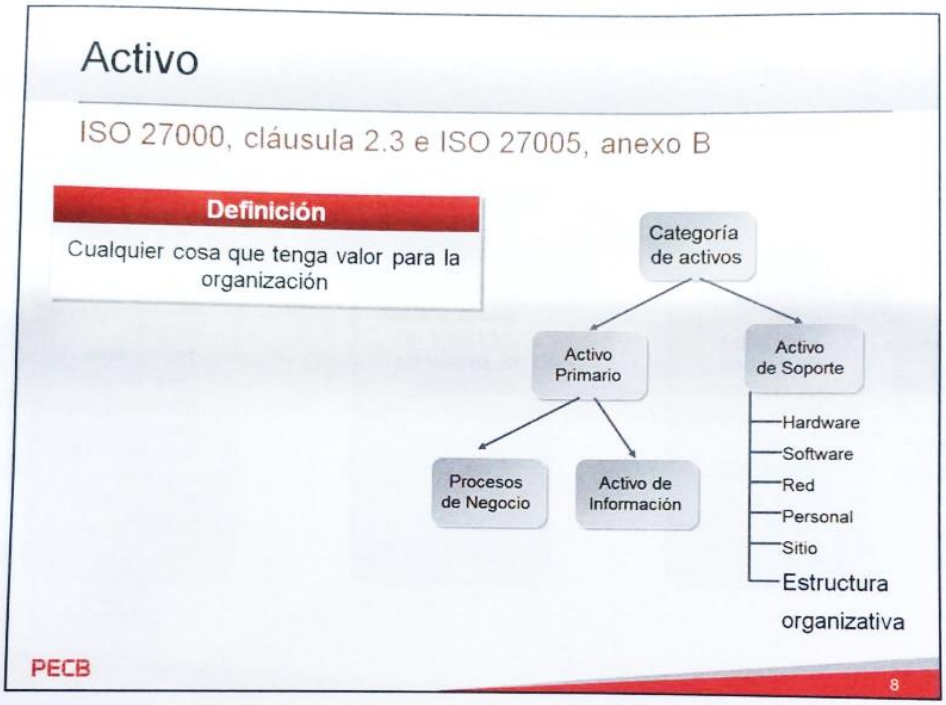
Existen varios modelos que se han desarrollado para analizar y comprender el contexto estratégico de la organización. Tenga en cuenta que este paso no se convierta en un proyecto en sí mismo. En la mayoría de las organizaciones, se han llevado a cabo estudios internamente o por empresas consultoras sobre su posicionamiento estratégico. Debería ser suficiente sólo recoger estos estudios, analizarlos y entrevistar a algunos actores clave para garantizar una comprensión adecuada de la organización.

Aquí están algunos modelos:

Análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas): este modelo realiza un diagnóstico de la organización, analizando sus fortalezas, debilidades, oportunidades y amenazas con el fin de formular opciones de política y determinar los puntos donde la organización debe invertir sus recursos (¿Tomar ventaja de las oportunidades? ¿Reducir sus debilidades? ¿Hacer frente a las amenazas?

Análisis STEP (Social, Tecnológico, Económico, Político) El análisis STEP le permite a la organización analizar las fuerzas del mercado y las oportunidades clasificadas en cuatro áreas: social, tecnológica, económica y política. Algunos autores han añadido otras dos categorías: legal y ambiental.

Anexo de libro: Sección 6, Pág. 8

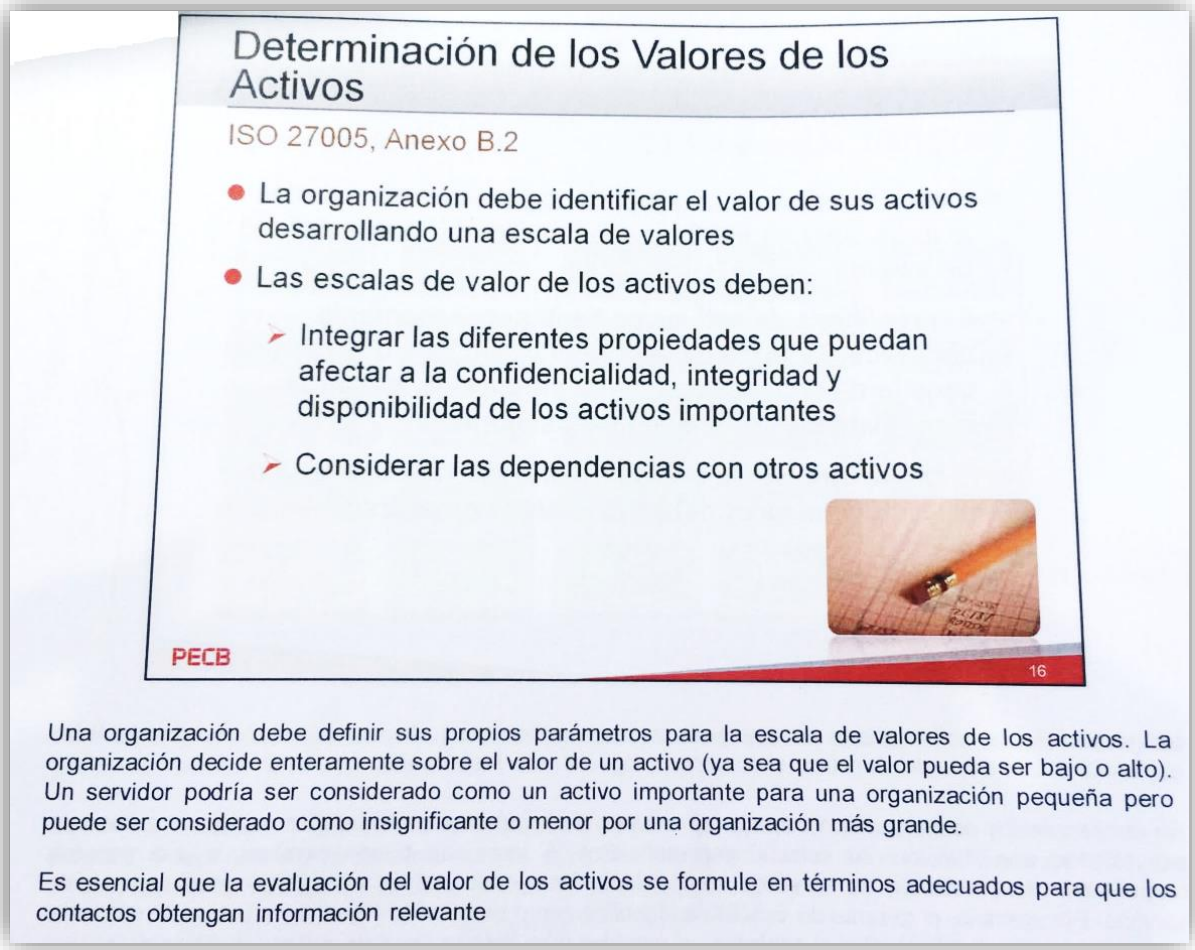


Un activo es cualquier cosa que sea de valor para la organización y por lo tanto necesita ser protegida. Para la identificación de los activos, se debe tener en cuenta que **un sistema de información consiste en mucho más que sólo el equipo físico y el software.** ISO 27005 divide los bienes en dos grandes categorías:

1. **Los activos principales** consisten en procesos de negocio y activos de información. Estos son los principales activos que tienen la mayor importancia para tener en cuenta en el análisis de riesgos y no los activos de apoyo como los servidores, por ejemplo.

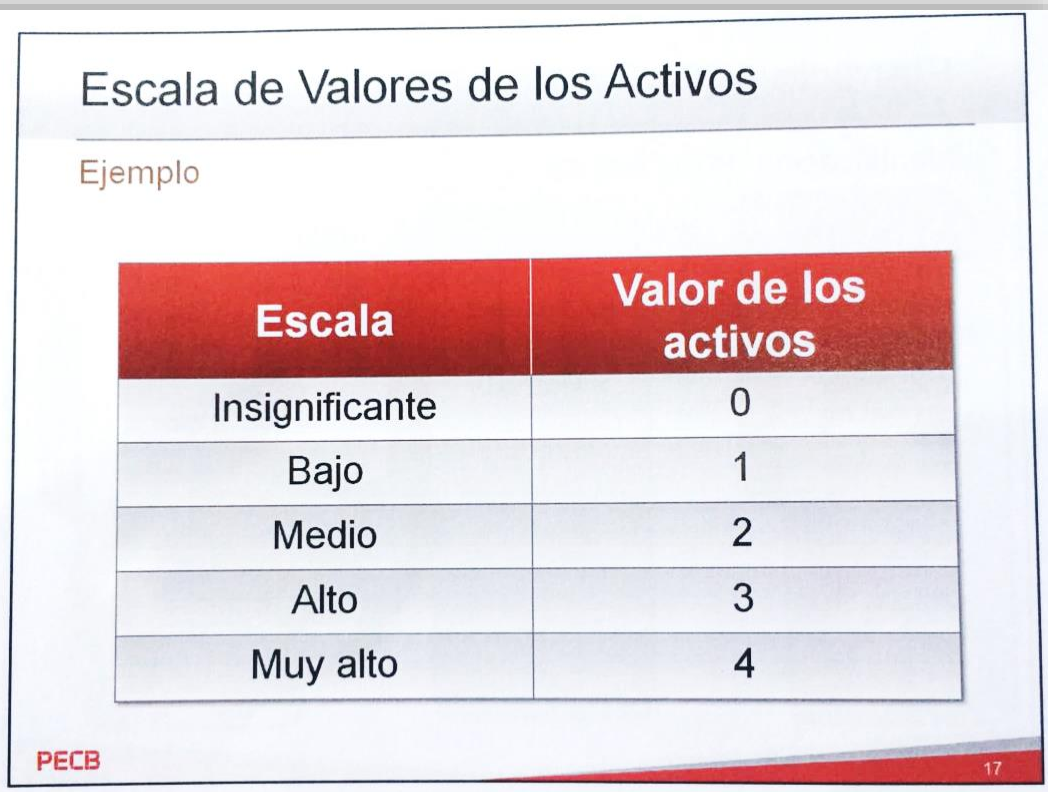
2. **Los activos de apoyo** incluyen el hardware, software, redes informáticas, el personal, los sitios y las estructuras organizativas.

Anexo de libro: Sección 6, Pág. 16-17



Una organización debe definir sus propios parámetros para la escala de valores de los activos. La organización decide enteramente sobre el valor de un activo (ya sea que el valor pueda ser bajo o alto). Un servidor podría ser considerado como un activo importante para una organización pequeña pero puede ser considerado como insignificante o menor por una organización más grande.

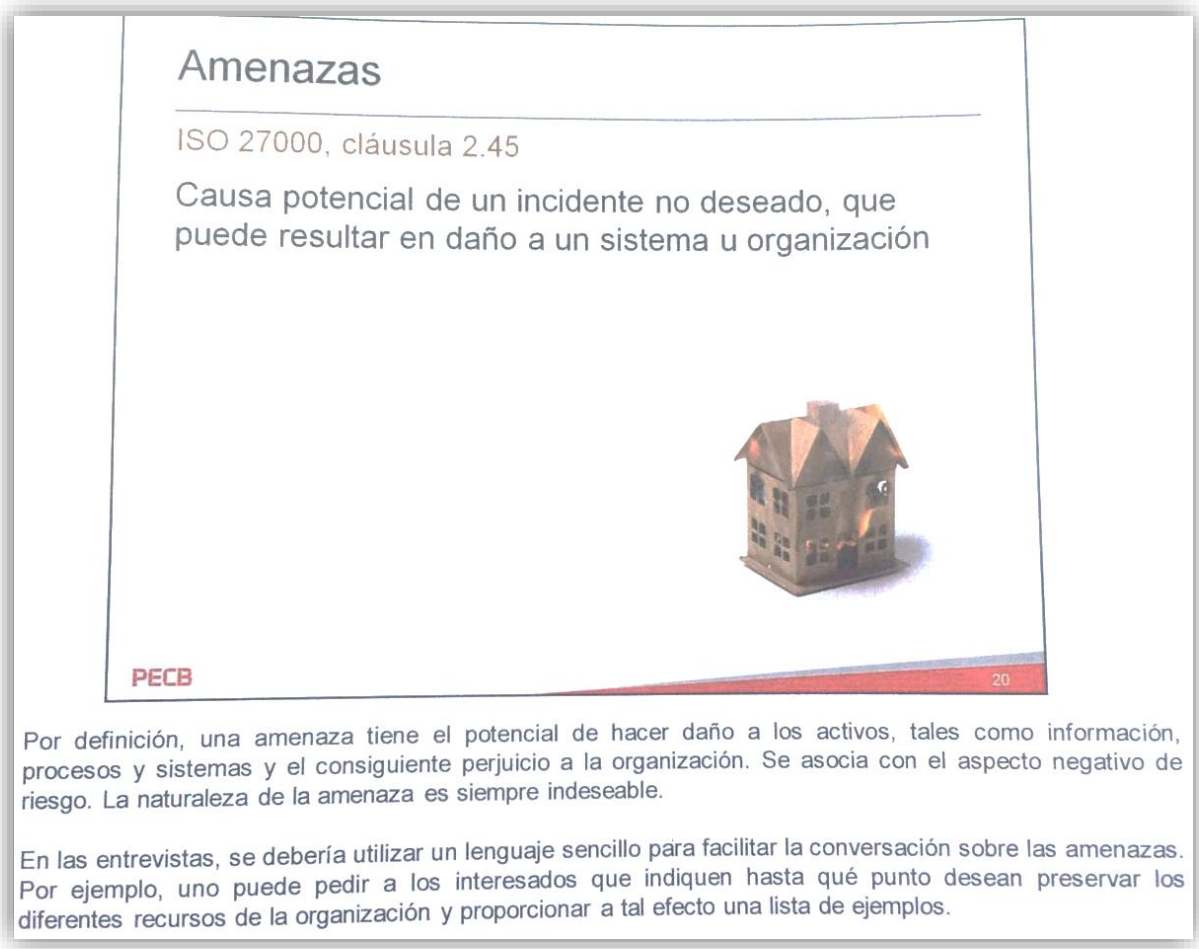
Es esencial que la evaluación del valor de los activos se formule en términos adecuados para que los contactos obtengan información relevante



Ejemplos de las escalas de valores de los activos:

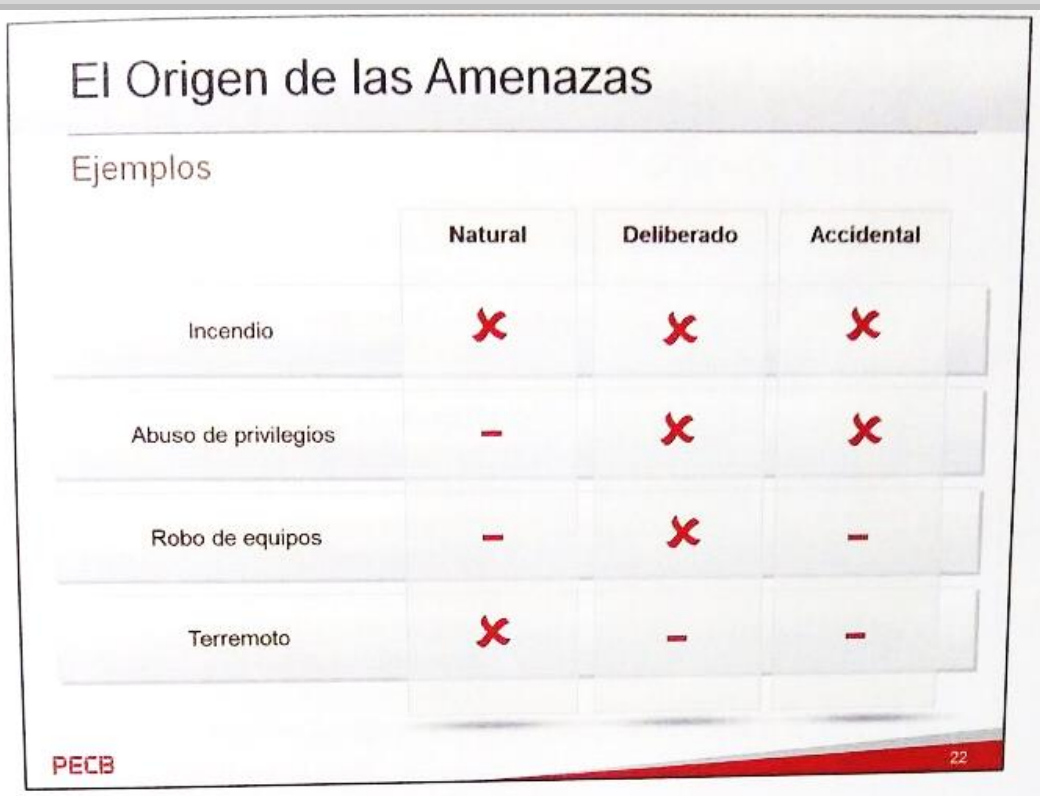
- Una gama de alto nivel que va de bajo a medio y a alto
- Un nivel más granular, distinguiendo entre insignificante, bajo, medio, alto y muy alto

Anexo de libro: Sección 6, Pág. 20,21, 22



Por definición, una amenaza tiene el potencial de hacer daño a los activos, tales como información, procesos y sistemas y el consiguiente perjuicio a la organización. Se asocia con el aspecto negativo de riesgo. La naturaleza de la amenaza es siempre indeseable.

En las entrevistas, se debería utilizar un lenguaje sencillo para facilitar la conversación sobre las amenazas. Por ejemplo, uno puede pedir a los interesados que indiquen hasta qué punto desean preservar los diferentes recursos de la organización y proporcionar a tal efecto una lista de ejemplos.



Las amenazas pueden tener un origen natural o humano, y pueden ser accidentales o deliberadas. Una amenaza puede surgir desde dentro o fuera de la organización.

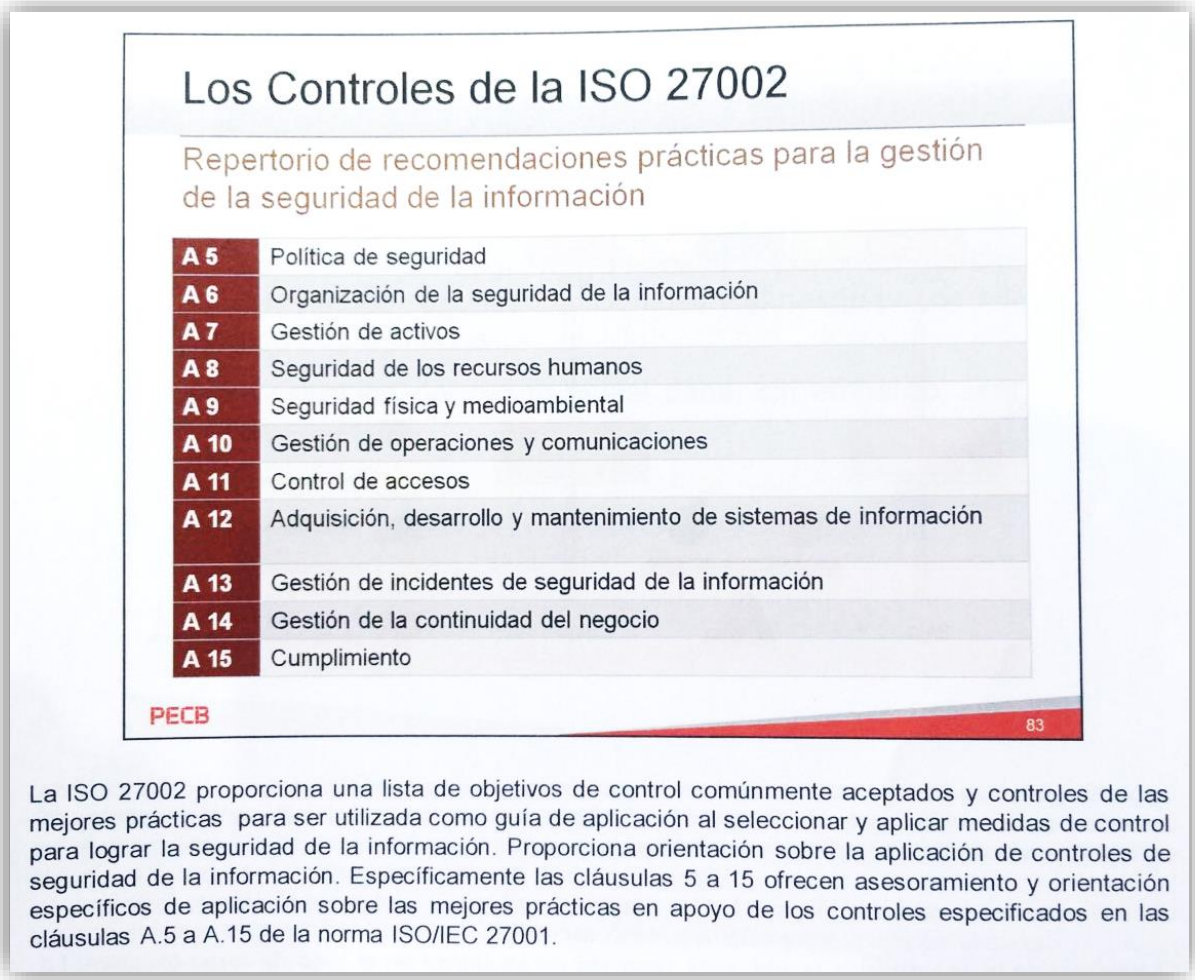
Las fuentes de las amenazas deberían ser identificadas, en particular aquellas que son deliberadas. La identificación de la fuente permite analizar con mayor detalle las características de una amenaza y cómo seleccionar tratamientos adecuados para protegerse de ella.

Tipos de Amenazas

ISO 27005, Anexo C

Tipo de amenaza
1 Daños físicos
2 Desastres naturales
3 Pérdida de servicio esencial
4 Trastornos causados por la radiación
5 Información comprometida
6 Fallos técnicos
7 Acción no autorizada

Anexo de libro: Sección 9, Pág. 83



Los Controles de la ISO 27002

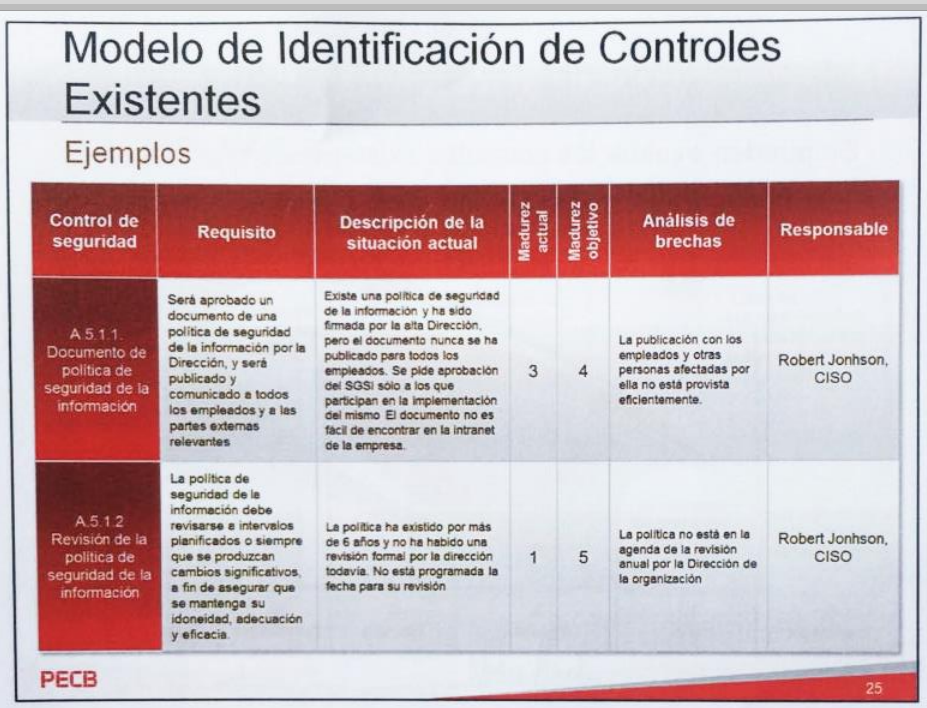
Repertorio de recomendaciones prácticas para la gestión de la seguridad de la información

A 5	Política de seguridad
A 6	Organización de la seguridad de la información
A 7	Gestión de activos
A 8	Seguridad de los recursos humanos
A 9	Seguridad física y medioambiental
A 10	Gestión de operaciones y comunicaciones
A 11	Control de accesos
A 12	Adquisición, desarrollo y mantenimiento de sistemas de información
A 13	Gestión de incidentes de seguridad de la información
A 14	Gestión de la continuidad del negocio
A 15	Cumplimiento

PECB 83

La ISO 27002 proporciona una lista de objetivos de control comúnmente aceptados y controles de las mejores prácticas para ser utilizada como guía de aplicación al seleccionar y aplicar medidas de control para lograr la seguridad de la información. Proporciona orientación sobre la aplicación de controles de seguridad de la información. Específicamente las cláusulas 5 a 15 ofrecen asesoramiento y orientación específicos de aplicación sobre las mejores prácticas en apoyo de los controles especificados en las cláusulas A.5 a A.15 de la norma ISO/IEC 27001.

Anexo de libro: Sección 6, Pág. 25



Modelo de Identificación de Controles Existentes

Ejemplos

Control de seguridad	Requisito	Descripción de la situación actual	Madurez actual	Madurez objetivo	Análisis de brechas	Responsable
A.5.1.1. Documento de política de seguridad de la información	Será aprobado un documento de una política de seguridad de la información por la Dirección, y será publicado y comunicado a todos los empleados y a las partes externas relevantes	Existe una política de seguridad de la información y ha sido firmada por la alta Dirección, pero el documento nunca se ha publicado para todos los empleados. Se pide aprobación del SGSI sólo a los que participan en la implementación del mismo. El documento no es fácil de encontrar en la intranet de la empresa.	3	4	La publicación con los empleados y otras personas afectadas por ella no está provista eficientemente.	Robert Jonhson, CISO
A.5.1.2 Revisión de la política de seguridad de la información	La política de seguridad de la información debe revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.	La política ha existido por más de 6 años y no ha habido una revisión formal por la dirección todavía. No está programada la fecha para su revisión	1	5	La política no está en la agenda de la revisión anual por la Dirección de la organización	Robert Jonhson, CISO

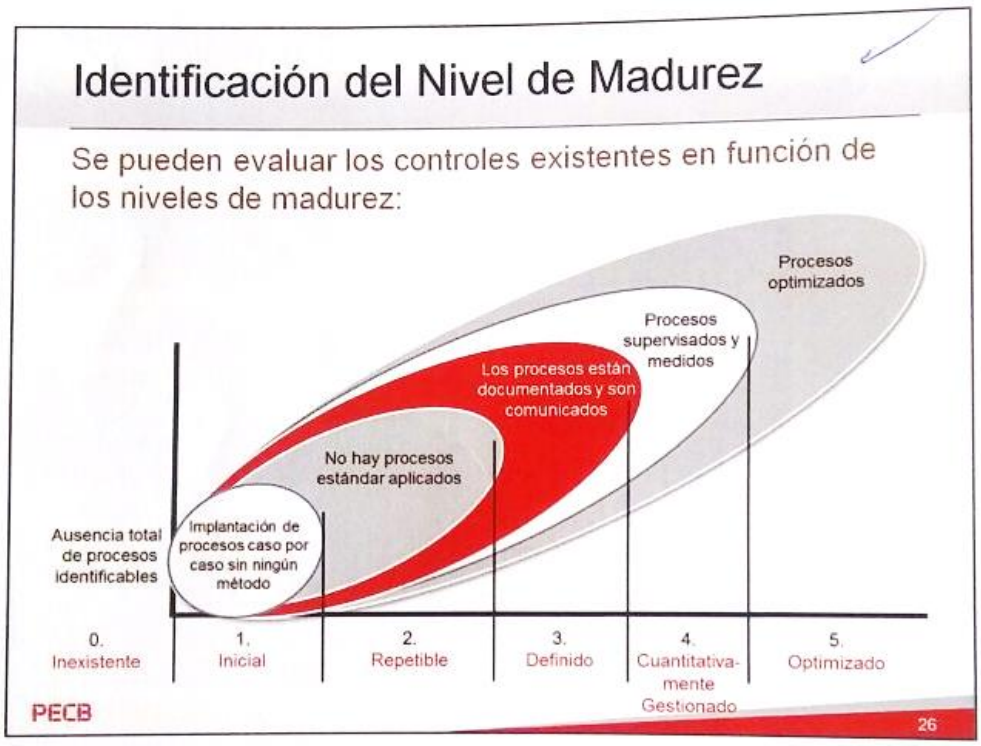
PECB 25

Para la identificación de los controles de seguridad existentes y previstos, se puede utilizar la lista de controles de seguridad de la norma ISO 27002 (o en el Anexo A de la ISO 27001). Esto ayuda a obtener una visión general de la situación existente en relación con las mejores prácticas de seguridad.

Para reunir la información adecuada en la organización, lo siguiente puede ser útil:

- El examen de los documentos que contienen información sobre los controles de seguridad (proceso de gestión de la seguridad, procedimientos, descripción de los controles de seguridad, informes de seguridad, etc.)
- Entrevista con los responsables de seguridad de la información y las personas que manejan las operaciones diarias relacionadas con los controles de seguridad.
- Revisar el sitio de los controles de seguridad física.
- Revisar los resultados de las auditorías internas

Anexo de libro: Sección 6, Pág. 26



0. Inexistente: Ausencia total de procesos identificables. La empresa no es consciente de que este es un problema para ser estudiado.

1. Inicial: Es evidente que la empresa es consciente de la existencia del problema y la necesidad de estudiarlo. Sin embargo, no hay un proceso estandarizado, pero los planteamientos en este sentido tienden a ser aplicados individualmente o en una base de caso por caso. No hay un enfoque global organizado por la gerencia.

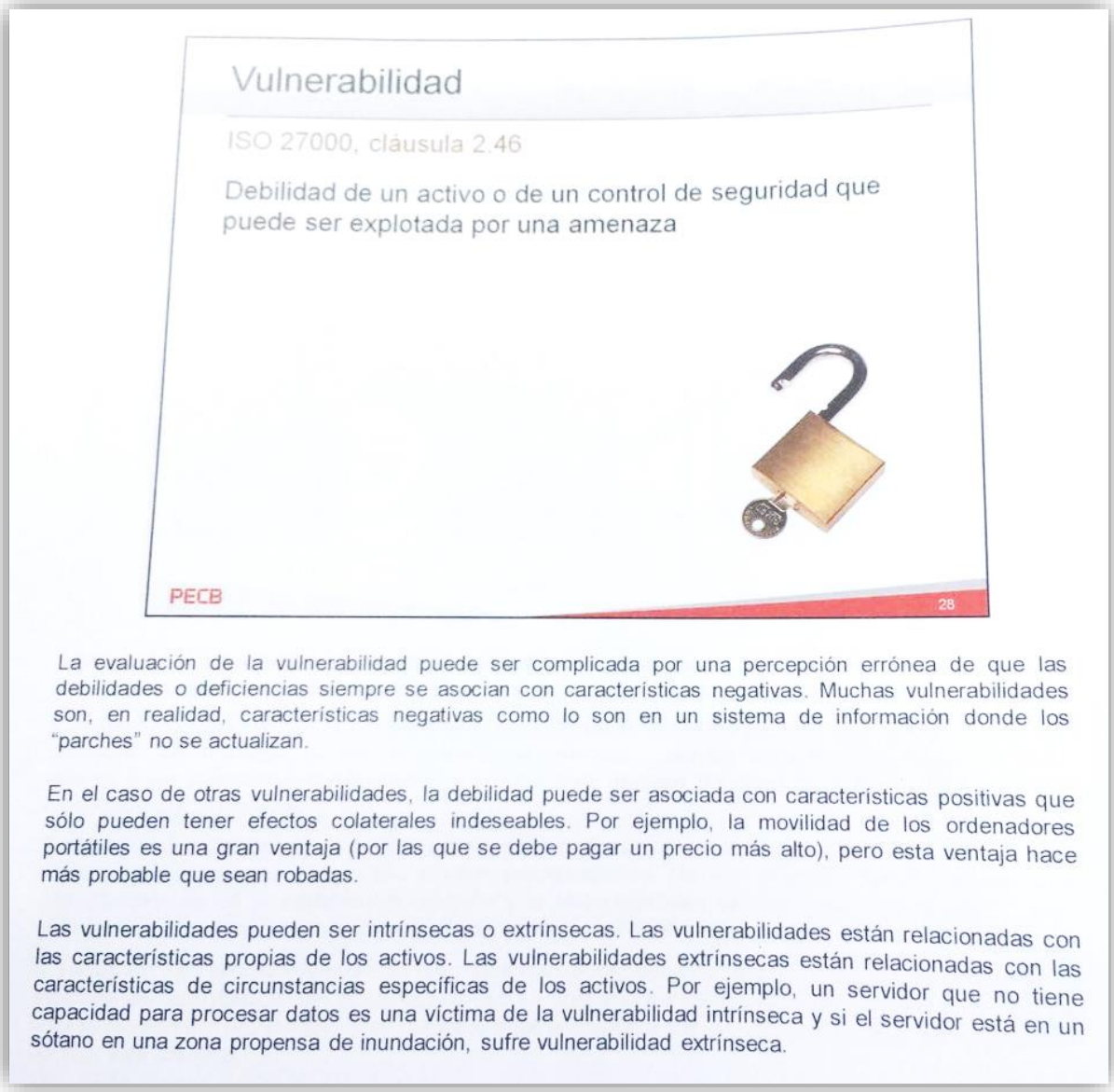
2. Gestionado: Los procesos se han desarrollado hasta una fase en la que diferentes personas que realizan la misma tarea utilizan los mismos procedimientos. No hay ninguna capacitación formal o comunicación de los procedimientos estándar y la responsabilidad se deja a la persona. Depende en gran medida del conocimiento personal, donde existe la probabilidad de error.

3. Definido: Los procedimientos han sido estandarizados, documentados y comunicados a través de sesiones de capacitación. Sin embargo, su uso se deja a la iniciativa individual, y es probable que los errores puedan ser detectados . Con respecto a los procedimientos, no son sofisticados, pero formalizan las prácticas existentes.

4. Cuantitativamente Gestionado: Es posible controlar y medir el cumplimiento de los procedimientos y tomar medidas donde los procesos no parecen funcionar correctamente. Los procesos se mejoran constantemente y corresponden a las buenas prácticas. La automatización y el uso de herramientas aún son limitados o parciales.

5. Optimizado: El proceso ha alcanzado el nivel de las mejores prácticas, a raíz de una mejora constante en comparación con los de otras organizaciones (Modelo de Madurez). El ordenador se utiliza como una forma de automatizar procesos de trabajo integrados, ofreciendo herramientas que mejoran la calidad y la eficiencia, y hacen que la empresa se adapte rápidamente.

Anexo de libro: Sección 6, Pág. 28

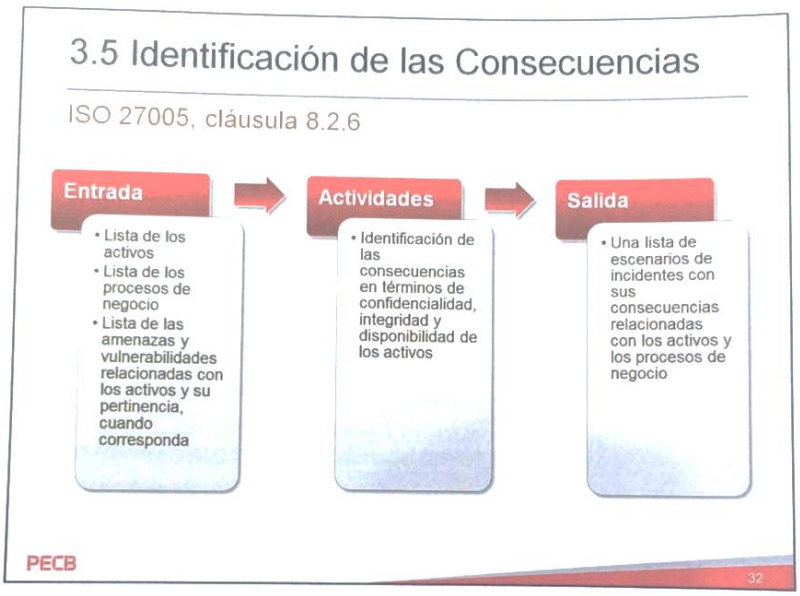


La evaluación de la vulnerabilidad puede ser complicada por una percepción errónea de que las debilidades o deficiencias siempre se asocian con características negativas. Muchas vulnerabilidades son, en realidad, características negativas como lo son en un sistema de información donde los "parches" no se actualizan.

En el caso de otras vulnerabilidades, la debilidad puede ser asociada con características positivas que sólo pueden tener efectos colaterales indeseables. Por ejemplo, la movilidad de los ordenadores portátiles es una gran ventaja (por las que se debe pagar un precio más alto), pero esta ventaja hace más probable que sean robadas.

Las vulnerabilidades pueden ser intrínsecas o extrínsecas. Las vulnerabilidades están relacionadas con las características propias de los activos. Las vulnerabilidades extrínsecas están relacionadas con las características de circunstancias específicas de los activos. Por ejemplo, un servidor que no tiene capacidad para procesar datos es una víctima de la vulnerabilidad intrínseca y si el servidor está en un sótano en una zona propensa de inundación, sufre vulnerabilidad extrínseca.

Anexo de libro: Sección 6, Pág. 32 y Pág. 35



El último paso de la identificación del riesgo es la identificación de los impactos sobre la organización que pueden ser causados por un escenario de incidentes. Un escenario de incidentes es la descripción de una amenaza que aprovecha una vulnerabilidad o un conjunto de vulnerabilidades en términos de seguridad de la información.

El impacto de los escenarios de incidentes se determina utilizando los criterios de impacto definidos durante la fase de establecimiento del contexto. Un impacto puede afectar a uno o más activos o parte de un activo. El impacto sobre los activos se puede calcular en valor financiero o por referencia a una escala cualitativa. Estas consecuencias pueden ser temporales o permanentes, como es el caso de la destrucción de un activo.


Identificación de las Consecuencias
Ejemplos
Disponibilidad
Degradación del Rendimiento
Interrupción del servicio
Inaccesibilidad de los servicios
Interrupción de las operaciones
Integridad
Cambio accidental
Modificación deliberada
Resultados incorrectos
Resultados incompletos
Pérdida de datos
Confidencialidad
Violación de la privacidad de los usuarios o clientes
Violación de la privacidad del personal de la organización
Divulgación de información confidencial
PECB
35

Anexo de libro: Sección 7, Pág. 42

ISO 31000, cláusula 5.4.3: Análisis del riesgo

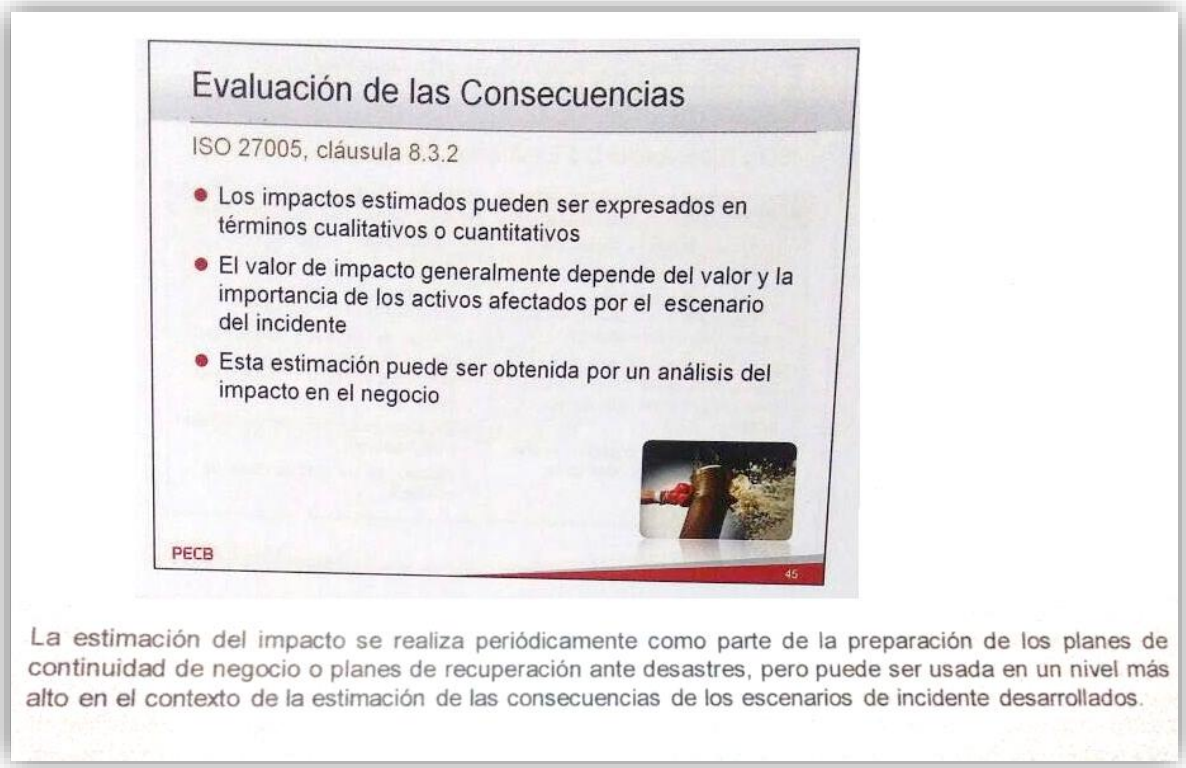
El análisis del riesgo implica desarrollar una comprensión del riesgo. El análisis del riesgo proporciona elementos de entrada para la evaluación del riesgo y para tomar decisiones acerca de si es necesario tratar los riesgos, así como sobre las estrategias y los métodos de tratamiento del riesgo más apropiados. El análisis del riesgo también puede proporcionar elementos de entrada para tomar decisiones cuando se deben hacer elecciones, y las opciones implican diferentes tipos de niveles de riesgo.

El análisis del riesgo implica la consideración de las causas y las fuentes del riesgo, sus consecuencias positivas y negativas, y la probabilidad de que estas consecuencias puedan ocurrir. Se deberían identificar los factores que afectan a las consecuencias y a la probabilidad. El riesgo se analiza determinando las consecuencias y su probabilidad, así como otros atributos del riesgo. Un suceso puede tener múltiples consecuencias y puede afectar a múltiples objetivos. También se deberían tener en cuenta los controles existentes, así como su eficacia y su eficiencia.

La forma de expresar las consecuencias y la probabilidad, así como la manera en que éstas se combinan para determinar un nivel de riesgo, debería corresponder al tipo de riesgo, a la información disponible y al objetivo para el que se utiliza el resultado de la apreciación del riesgo. Todos estos datos deberían ser coherentes con los criterios de riesgo. También es importante considerar la interdependencia de los diferentes riesgos y de sus fuentes.

La confianza en la determinación del nivel de riesgo y su sensibilidad a las condiciones previas y a las hipótesis se debería considerar en el análisis y comunicar de manera eficaz a las personas que han de tomar decisiones y, cuando corresponda, a otras partes interesadas. Factores tales como las diferencias de opinión entre expertos, la incertidumbre, la disponibilidad, la calidad, la cantidad y la validez de la pertinencia de la información, o las limitaciones respecto a modelos establecidos se deberían indicar y pueden resaltarse.

Anexo de libro: Sección 7, Pág. 44



La estimación del impacto se realiza periódicamente como parte de la preparación de los planes de continuidad de negocio o planes de recuperación ante desastres, pero puede ser usada en un nivel más alto en el contexto de la estimación de las consecuencias de los escenarios de incidente desarrollados.